

DE VERWERKING VAN PERSOONSgegevens IN DE BANKSECTOR

De invloed van de Wet van 8 december 1992¹⁷⁹

Koen Van Raemdonck

Onder wetenschappelijke begeleiding van
Prof. dr. H. Braeckmans

V. GRENDOERSCHRIJDEND VERKEER VAN PERSOONS- gegevens

De internationalisering van de economie genereert een toenemend aantal bankverrichtingen met een grensoverschrijdend karakter. Dit impliceert het ontstaan van een permanent grensoverschrijdend gegevensverkeer in de banksector. Een adequate wetgeving inzake persoonsgegevensbescherming zou op dit fenomeen moeten inspelen.

De Belgische WVP regelt het internationaal gegevensverkeer eerder incidenteel en vooral summier. Incidenteel wordt ingespeeld op deze ontwikkelingen door art. 3 WVP dat het toepassingsgebied van de WVP regelt. De Privacywet is van toepassing op manuele bestanden op Belgisch grondgebied (art. 3 §1 WVP). Voor automatische verwerkingen is er echter een probleem van situering.¹⁸⁰ Daarom bepaalt art. 3 §1 2° WVP dat de wet toepasselijk is wanneer de verwerking direct toegankelijk is in België aan de hand van middelen die eigen zijn aan de verwerking, zelfs al gebeurt het geheel of een deel van de bewerkingen in het buitenland. Deze bepaling is niet zonder belang voor de banksector, waar verscheidene banken buitenlandse filialen hebben, waarvan de verwerkingen via computernetwerken rechtstreeks toegankelijk zijn in België. De WVP is dan van toepassing op de daarin verwerkte persoonsgegevens.¹⁸¹

De WVP verbiedt ook de verzameling met het oog op verwerking in het

¹⁷⁹ Het eerste deel is reeds verschenen in *Jura Falc.* 1996-97, 649-690.

¹⁸⁰ M.-H. BOULANGER, C. DE TERWANGE en Th. LEONARD, "La protection de la vie privée à l'égard de données à caractère personnel", *J.T.* 1993, 374; P. LEMMENS, "Informatique et protection de la vie privée: la loi du 8 décembre 1992" in X. (ed.), *Droit de l'informatique*, Brussel, Editions du Jeune Barreau, 1993, 417-418.

¹⁸¹ Voor kritiek op art. 3 §1 2° WVP, zie X., *De bescherming van de persoonlijke levenssfeer: toepassing van de wet van 8 december 1992 in de banksector*, Brussel, Belgische Vereniging van Banken, (Reeks aspecten en documenten nr. 146), 1993, 16.

buitenland van die persoonsgegevens waarvan de verwerking in België niet is toegestaan op grond van de artikelen 6, 7 en 8 WVP.¹⁸²

Indien bij een persoon op Belgisch grondgebied persoonsgegevens worden verzameld met het oog op de verwerking ervan buiten het grondgebied, moet die persoon in kennis worden gesteld van hetgeen bepaald is in art. 4 §1 1° tot 5° WVP, behoudens wanneer het gaat om verwerkingen van persoonsgegevens met het oog op het bedoelde in art. 11 2° tot 5° WVP.

De drie voorgaande bepalingen die overigens niet expliciet het grensoverschrijdend verkeer van persoonsgegevens betreffen, geven aan de WVP een duidelijke transnationale werking.

Hoofdstuk VI van de WVP besteedt dan expliciet, doch zeer summier¹⁸³, aandacht aan het grensoverschrijdend verkeer van gegevens. Art. 22 WVP bepaalt dat, onverminderd de internationale overeenkomsten waarbij België partij is, de overdracht van verwerkte persoonsgegevens in enigerlei vorm tussen het Belgisch grondgebied en het buitenland, hetzij verboden kan worden, hetzij onderworpen kan worden aan een voorafgaande vergunning, hetzij gereguleerd kan worden met het oog op de vrijwaring van het recht op eerbiediging van de persoonlijke levenssfeer. De verdere uitwerking hiervan moet bij K.B. gebeuren. Een dergelijk K.B. ex art. 22 WVP kwam tot op heden nog niet tot stand. Nochtans is art. 22 WVP vast en zeker een basis voor eventuele reglementeringen die de overdracht van gegevens naar landen die terzake de bescherming van persoonsgegevens geen wetgeving bezitten, kunnen beperken of verbieden.

Bij het beperken van het grensoverschrijdend verkeer van persoonsgegevens zal België rekening moeten houden met zijn verdragsverplichtingen terzake.

Zo bepaalt art. 12 tweede lid van de Conventie nr. 108 van de Raad van Europa tot bescherming van personen t.o.v. de geautomatiseerde verwerking van persoonsgegevens dat de partijen bij de Conventie zich ertoe verbinden om onderling geen beperkingen te stellen aan de overdracht van gegevens enkel en alleen ten behoeve van de bescherming van de persoonlijke levenssfeer.¹⁸⁴ De Conventie bevat wel een uitzondering voor bepaalde categorieën van persoonsgegevens waarvoor de nationale wet een speciale behandeling voorschrijft en voor wat betreft de gegevensuitvoer naar landen die geen partij zijn bij de Conventie via een staat die wel partij is bij de Conventie (art. 12 derde lid).¹⁸⁵ Beperkingen aan de vrije gegevensoverdracht naar landen die

¹⁸² M.a.w. verbiedt art. 4 §2 WVP de verwerking in het buitenland van in België verzamelde gevoelige gegevens s.l.

¹⁸³ Slechts één artikel wordt aan dit probleem gewijd, namelijk art. 22 WVP.

¹⁸⁴ Conventie Raad van Europa tot bescherming van personen t.o.v. de geautomatiseerde verwerking van persoonsgegevens, goedgekeurd bij Wet 17 juni 1991, B.S. 30 december 1993.

¹⁸⁵ Zie hierover J. DUMORTIER, *Europese en Belgische reglementering over de behandeling van*

geen partij zijn en die (naar Belgisch oordeel) geen afdoende persoonsgegevensbescherming hebben, vallen buiten het toepassingsgebied van de Conventie.

Art. 25 van de Richtlijn reglementeert het doorgeven van persoonsgegevens van een lidstaat naar een derde land. De centrale eis die gesteld wordt opdat een dergelijke doorgifte toelaatbaar zou zijn, luidt dat het land van bestemming een passend beschermingsniveau moet waarborgen. Dit strenge principe wordt sterk getemperd (uitgehoud?) door de waslijst van uitzonderingen van art. 26 van de Richtlijn. Een aantal van die uitzonderingen lijkt relevant voor de banksector. De Richtlijn is echter nog niet geïmplementeerd.

De Richtlijn is ook duidelijk t.a.v. het verkeer van persoonsgegevens tussen de lidstaten onderling. Art. 1 tweede lid van de Richtlijn bepaalt immers dat de lidstaten het vrij verkeer van persoonsgegevens tussen hen niet mogen beperken noch verbieden om redenen die verband houden met de bescherming van de persoonlijke levenssfeer. De Richtlijn moet op dit punt m.i. zo geïnterpreteerd worden dat ze aan de Lid-Staten het verbod oplegt om Privacyregulering te gebruiken op een wijze die neerkomt op een maatregel van gelijke werking als kwantitatieve in- of uitvoerbeperking in de zin van art. 30 of art. 34 EG-Verdrag. De Richtlijn gaat er daarbij terecht van uit dat persoonsgegevens goederen zijn (vb. verkoop van adressen door marketingbureaus). Dit sluit aan bij de economische realiteit. Nu gegevens ook als goederen worden beschouwd, dient het vrij verkeer van goederen hier te worden vertaald als een vrij verkeer van persoonsgegevens.

VI. CONTROLE EN TOEZICHT

A. DE STAAT

Art. 16 §1 WVP legt aan de houder van het bestand de verplichting op om voor elke verwerking een staat op te maken. Deze staat moet vermelden welke de aard van de verwerkte gegevens is, wat het doel van de verwerking is, of er onderlinge verbindingen, verbanden of raadplegingen voorhanden zijn, alsmede de personen of categorieën van personen aan wie de persoonsgegevens worden doorgegeven.

De bestaansreden van deze staat is duidelijk; om te kunnen nagaan of de houder de WVP heeft overtreden, is het noodzakelijk dat men juist en onbetwistbaar kan nagaan welke finaliteit(en) hij heeft vooropgesteld. De staat is dus een instrument dat behoorlijke toetsing moet mogelijk maken.

B. DE AANGIFTE

persoonsgegevens, Leuven, ICRI, 1993, 7-9.

Art. 17 §1 WVP bepaalt dat iedere houder, alvorens een geautomatiseerde verwerking van persoonsgegevens op te starten, daarvan eerst bij de CBPL aangifte moet doen. Art. 17 §3 WVP bepaalt uitdrukkelijk welke gegevens de aangifte moet vermelden.¹⁸⁶ Zo moet onder meer gemeld worden aan welke personen of categorieën van personen de persoonsgegevens zullen meegegeed worden (art. 17 §3 7° WVP) en welke waarborgen aan de mededeling verbonden zijn (art. 17 §3 8° WVP).

De aangifte gebeurt met een tweevoudige doelstelling: informatie voor de verwerkte personen en informatie voor de CBPL.¹⁸⁷ De aangifte zal in dat opzicht belangrijk zijn om de naleving van het finaliteitsbeginsel te verzekeren. Zowel voor de banken als voor de CBPL zelf betekent art. 17 WVP echter een loodzware administratieve last. Voorstellen werden dan ook gedaan om de aangifte te beperken tot een aantal cruciale gegevens.¹⁸⁸ Op voorstel van de CBPL werd in een K.B.¹⁸⁹ daarom getracht deze administratieve last iets te verlichten. Allereerst werden er modelformulieren en lexica van vooraf gedefinieerde doeleinden in het Belgisch Staatsblad gepubliceerd. Deze modelformulieren peilen systematisch naar de informatie-elementen van art. 17 §3 en §6 WVP. Wat de doeleinden betreft, werd in overleg met de banksector een lexicon opgesteld waarin de meest voorkomende doeleinden gedefinieerd werden. Het lexicon is echter noch exhaustief, noch bindend voor de banken. Het biedt wel een voordeel van snelheid; door de gsystematiseerde aanpak is men zeker van een precieze en volledige aangifte. De artikelen 2 tot 4 van het K.B. nr. 12 i.v.m. de bijdrage die aan de CBPL moet worden gestort bij de aangifte van de verwerking van persoonsgegevens, werden intussen gewijzigd door de artikelen 1 tot 3 van het K.B. nr. 12bis.¹⁹⁰ Tegen het K.B. nr. 12 was veel kritiek gerezen; allereerst waren de tarieven nominaal te hoog.¹⁹¹ Voorts bleek het criterium van de belangrijkheid van de verwerking ter bepaling van de hoogte van de bijdrage onwerkbaar. Tenslotte ondermijnde de tariefstructuur het wezen van de WVP. Men is immers een bijdrage verschuldigd per aangifte (dus per verwerking), wat aanleiding gaf tot het steeds verruimen van de doeleinden van de verwerking.¹⁹² Gedeeltelijk is men in het K.B. nr. 12bis tegemoet gekomen aan

¹⁸⁶ Zie daarover in extenso: E. MEYSMANS, "De aangifte" in X. (ed.), *De Wet tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens*, Brussel, Belgische Vereniging van Banken, 1993, 1-12; M.-H. BOULANGER, C. DE TERWANGE en Th. LEONARD, *l.c.*, 381-382; P. LEMMENS, *l.c.*, 419-420; S. GUTWIRTH, *o.c.*, 1466-1468.

¹⁸⁷ Zie E. MEYSMANS, *l.c.*, 1.

¹⁸⁸ Zie hierover: M.-H. BOULANGER, C. DE TERWANGE en Th. LEONARD, *l.c.*, 382.

¹⁸⁹ K.B. nr. 12, 7 maart 1995 tot vaststelling van de bedragen die aan de Commissie voor de Bescherming van de Persoonlijke Levenssfeer moeten worden gestort bij de aangifte van de verwerking van persoonsgegevens, *B.S.* 14 maart 1995.

¹⁹⁰ K.B. nr. 12 bis van 12 maart 1996 tot wijziging van het K.B. nr. 12 van 7 maart 1995 tot vaststelling van de bedragen die aan de CBPL moeten worden gestort bij de aangifte van de verwerking van persoonsgegevens, *B.S.* 15 maart 1996, 5801-5802.

¹⁹¹ 7000, 8000 of 10.000 frank al naargelang de aangifte elektronisch, op modelpapier of vrij gebeurde.

¹⁹² Zie hierover Advies nr. 32/95 van 22 december 1995 van de CBPL, *B.S.* 15 maart 1996.

bovenstaande kritiek. Voortaan betaalt men nog slechts vijfduizend frank voor een aangifte op modelpapier en duizend frank voor een elektronische aangifte (de artikelen 1 en 2 van het K.B. nr. 12bis). Voor de verwerkingen die op minder dan honderd personen betrekking hebben, betaalt men slechts de helft van bovenvermelde bedragen. Op deze wijze werd het criterium van de belangrijkheid van de verwerking ter bepaling van de bijdrage gekwantificeerd.¹⁹³ Uiteindelijk is men niet afgestapt van het principe van één bijdrage per verwerking, hoewel het verslag aan de Koning, voorafgaand aan het K.B. nr. 12bis, ervoor pleitte om slechts één bijdrage te vragen, ongeacht het aantal tegelijk gedane aangiften van verwerkingen.¹⁹⁴ Op deze wijze beoogde men immers een grotere precisie te verkrijgen bij de aanduiding van de diverse doeleinden door het ontnemen van de financiële incentive om de doeleinden zo ruim mogelijk te definiëren. Blijkbaar is men ervan overtuigd dat met een louter nominale tariefwijziging men een zelfde resultaat zal bereiken. Wijziging van de oorspronkelijke aangifte kost voortaan achthonderd frank ongeacht het aantal wijzigingen (art. 3 van het K.B. nr. 12bis).

In uitvoering van art. 17 §8 WVP voorziet het K.B. nr 13 bovendien in de voorwaardelijke vrijstelling van de aangifteplicht van bepaalde soorten van geautomatiseerde verwerkingen die kennelijk geen gevaar inhouden op het gebied van de schending van de persoonlijke levenssfeer.¹⁹⁵ We verwijzen hier vooral naar de vrijstelling van aangifte bij de verwerking van persoonsgegevens met als finaliteit loonadministratie (art. 2), personeelsadministratie (art. 3), voeren van de boekhouding (art. 4), administratie van vennoten en aandeelhouders (art. 5), uitsluitend beheer van klanten of leveranciers (art. 6), de registratie van bezoeken in het kader van toegangscontrole (art. 9) en de residuaire categorie van verzameling van de voor communicatie noodzakelijke identificatiegegevens (art. 8). Bijna steeds wordt de vrijstelling gekoppeld aan een verbod op mededeling aan derden van die gegevens, alsook aan het vereiste dat de betrokken gegevens niet langer dan strikt noodzakelijk bewaard zouden blijven.¹⁹⁶ Dit systeem van voorwaardelijke vrijstellingen dient om een overstelping met aangiften te vermijden. Het aantal automatische verwerkingen loopt immers in de honderdduizenden. Een zekere selectiviteit inbouwen in de aangifteplicht zelf moet de informatie- en controlefunctie van de aangifte garanderen. Wat kennelijk geen gevaar voor de persoonlijke levenssfeer oplevert, wordt weggezeefd.¹⁹⁷

¹⁹³ Formeel diende men immers het criterium van de belangrijkheid van de verwerking te behouden, in afwachting van een wijziging van art. 17 §9 WVP.

¹⁹⁴ Advies nr. 32/95 van 22 december 1995 van de CBPL, *B.S.* 15 maart 1996; Verslag aan de Koning, *B.S.* 15 maart 1996.

¹⁹⁵ K.B. nr. 13 van 12 maart 1996 tot voorwaardelijke vrijstelling van de aangifteplicht voor bepaalde soorten van geautomatiseerde verwerkingen van persoonsgegevens die kennelijk geen gevaar opleveren op het gebied van de schending van de persoonlijke levenssfeer, *B.S.* 15 maart 1996.

¹⁹⁶ Zie art. 6 in fine K.B. nr 13 voor een voorbeeld.

¹⁹⁷ Verslag aan de Koning, *B.S.* 15 maart 1996.

Ook de Richtlijn voorziet in art. 18 in een aangifte, "aanmelding" genaamd. Art. 19 bepaalt de inhoud daarvan; deze is gelijklopend met die van de Belgische WVP. Vrijstellingen zijn volgens het tweede lid van art. 18 mogelijk, op voorwaarde dat de nationale regelgeving de doeleinden van de verwerking, de verwerkte gegevens of categorieën van verwerkte gegevens, de categorieën betrokkenen, de ontvangers of categorieën van ontvangers aan wie de gegevens worden verstrekt, en de periode gedurende dewelke de gegevens worden bewaard, preciseert. Of bovenstaande elementen telkenmale voldoende gepreciseerd zijn in K.B. nr. 13, mag betwijfeld worden. Kan men de tekst "zolang als noodzakelijk voor doel x of y" beschouwen als een voldoende precisering van de periode gedurende welke de gegevens bewaard zullen worden? K.B. nr. 13 lijkt dan ook niet in volledige overeenstemming met de Richtlijn. Art. 21 derde lid van de Richtlijn schrijft bovendien voor dat, zelfs in geval van een vrijstelling, de houder toch aan ieder die erom verzoekt de inlichtingen, bedoeld in art. 19 eerste lid a) tot e), op passende wijze moet verstrekken. Deze laatste verplichting voor de houder is echter, ondanks het advies van de CBPL, niet opgenomen in K.B. nr. 13.¹⁹⁸ De Belgische regelgeving is dus ook op dit punt zeker niet richtlijnconform en vergt dus aanpassing tegen 1998.

Bij de CBPL wordt een register gehouden van geautomatiseerde verwerkingen van persoonsgegevens (art. 18 WVP). Het register moet de gegevens, bepaald in art. 17 §3 en §6 WVP, bevatten. De toegang tot het register door de betrokkenen moet geregeld worden in een K.B. en heeft tot doel dat de betrokkenen alle elementen, nodig voor uitoefening van hun rechten (zoals het recht op toegang en het recht op verbetering, resp. art. 10 en 12 WVP), op eenvoudige wijze kunnen consulteren.¹⁹⁹ Het identificatienummer van de verwerking in dat register moet vermeld staan op ieder stuk waarvoor ze gebruikt is (art. 20 in fine WVP). Met dit nummer kan de cliënt zich tot de CBPL wenden teneinde informatie over de verwerking op te vragen. Het vermelden van het identificatienummer op elk stuk betekent, in het bijzonder voor de banksector waar de cliënten een enorm aantal stukken (bv. afschriften) per jaar ontvangen, eens te meer een bijkomende administratieve kost. Het K.B. dat de inzage in het register praktisch moet regelen, is nog niet genomen. Ook Art. 21 derde lid van de Richtlijn schrijft de oprichting van een register voor.

C. DE COMMISSIE VOOR DE BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER

De CBPL werd in zijn huidige vorm opgericht door de artikelen 23 tot 36 WVP. Bij de totstandkoming van de WVP werd de bestaande CBPL, zoals die

¹⁹⁸ Advies nr. 33/95 van 22 december 1995 van de CBPL, *B.S.* 15 maart 1996.

¹⁹⁹ P. LEMMENS, *l.c.*, 435.

opgericht werd bij de Wet van 15 januari 1990 houdende de oprichting en de organisatie van een Kruispuntbank van de Sociale Zekerheid²⁰⁰ en zoals die in bevoegdheid werd uitgebreid door de Wet Consumentenkrediet en het K.B. van 20 november 1992 betreffende de verwerking van persoonsgegevens inzake het consumentenkrediet²⁰¹, opgeheven. De artikelen 23 tot 28 WVP regelen de samenstelling van de CBPL. Opvallend bij deze omstandige regeling, is het vereiste van pariteit tussen Nederlandstaligen en Franstaligen in de Commissie en het vereiste evenwicht in de samenstelling tussen de diverse sociaal-economische groepen.

De artikelen 29 tot 33 WVP regelen de diverse bevoegdheden van de CBPL.²⁰² De CBPL beschikt vooreerst over een advies- en aanbevelingsbevoegdheid omtrent iedere aangelegenheid die betrekking heeft op de toepassing van de grondbeginselen van de bescherming van de persoonlijke levenssfeer.²⁰³ Voorts heeft de CBPL de bevoegdheid de haar toegestuurde klachten te onderzoeken. De CBPL mag daarbij een beroep doen op de medewerking van deskundigen.²⁰⁴ De CBPL kan echter geen bindende beslissingen nemen; haar beslissingen hebben slechts een moreel gezag.²⁰⁵ Anderzijds kan de voorzitter van de CBPL wel elk geschil betreffende de WVP haar uitvoeringsmaatregelen aan de rechtbank van eerste aanleg voorleggen.²⁰⁶ Deze laatste kan natuurlijk wel bindend beslissen.

De artikelen 34 tot 36 WVP bevatten tenslotte een aantal administratieve bepalingen betreffende de werkingskosten van de CBPL en de vergoeding van de voorzitter en het secretariaat van de CBPL.

Besloten kan dus worden dat de CBPL naast een adviesorgaan, vooral een orgaan is dat tevens controle- en toezichtstaken vervult.

In de Richtlijn wordt, aangaande de adviserende taak, voorzien in de oprichting van een "groep voor de bescherming van personen in verband met de verwerking van persoonsgegevens" (art. 29). De precieze taken van deze groep worden verder gedefinieerd (art. 30). Voor wat betreft de controle- en toezichtstaken daarentegen, moet elk van de Lidstaten zelf voorzien in een "toezichthoudende autoriteit" waarvan de bevoegdheden ook verder bepaald zijn in de Richtlijn (art. 28). Dit onderscheid moet wellicht beschouwd worden als een juiste toepassing van het subsidiariteitsbeginsel. Controle en toezicht gebeuren het best op het niveau van de lidstaten, terwijl aanbevelingen best op

²⁰⁰ Wet van 15 januari 1990 houdende de oprichting en de organisatie van een Kruispuntbank van de sociale zekerheid, *B.S.* 22 februari 1990.

²⁰¹ K.B. van 20 november 1992 betreffende de verwerking van persoonsgegevens inzake consumentenkrediet, *B.S.* 11 december 1992.

²⁰² Voor een uitgebreide uiteenzetting hierover, zie: M.-H. BOULANGER, C. DE TERWANGE, en Th. LEONARD, *l.c.*, 385-387 en P. LEMMENS, *l.c.*, 439-441.

²⁰³ Voor de modaliteiten hiervan, zie de artikelen 29 en 30 WVP.

²⁰⁴ Voor de modaliteiten hiervan, zie de artikelen 31 tot 33 WVP.

²⁰⁵ P. LEMMENS, *l.c.*, 441.

²⁰⁶ Zie art. 32 §3 WVP.

het niveau van de Unie gebeuren.

D. DE STRAFRECHTELIJKE BETEUGELING IN DE WVP

Een regel is maar waard wat de beteugeling van de niet-naleving ervan waard is. Hoofdstuk VIII van de WVP bevat die sancties in de vorm van strafbepalingen.²⁰⁷ Wie de artikelen 4 tot en met 10 WVP, 17 tot en met 19 WVP, 21 tot en met 22 WVP of 32 WVP schendt, wordt gestraft met een boete van honderd tot honderdduizend frank (art. 39). Wie art. 15 of 16 WVP niet nakomt, wordt gestraft met een boete van honderd tot twintigduizend frank (art. 38). Wie art. 33 WVP niet nakomt, wordt gestraft met een boete van honderd tot tienduizend frank (art. 37).

Om de inning van de boete te verzekeren, is bepaald dat de houder van het bestand of zijn vertegenwoordiger in België burgerrechtelijk aansprakelijk is voor de betaling van de boeten waartoe zijn aangestelde of lasthebber is veroordeeld (art. 42).

De WVP bevat ook nog een aantal bijkomende straffen. Zo kan de rechter de publicatie van het vonnis in een of meer dagbladen bevelen (art. 40). De rechter kan voorts de verbeurdverklaring van de kwestieuze drager van persoonsgegevens uitspreken of de uitwissing van die gegevens gelasten (art. 41 §1). De rechter kan tenslotte ook voor ten hoogste twee jaar het verbod opleggen om rechtstreeks of onrechtstreeks het beheer te hebben over enige verwerking van persoonsgegevens (art. 41 §2). Schending van dit verbod wordt gestraft met een gevangenisstraf van drie maanden tot twee jaar en met een geldboete van honderd tot honderdduizend frank of met één van die straffen alleen (art. 41 §3).

In geval van herhaling van de misdrijven, bepaald in de artikelen 37, 38 of 39 WVP, voorziet de WVP een gevangenisstraf van drie maanden tot twee jaar en een boete van honderd tot honderdduizend frank of met één van die straffen alleen (art. 41 §3). Bovendien worden alle bepalingen van Boek I van het Strafwetboek van toepassing verklaard op de misdrijven die bepaald zijn in de WVP of zijn uitvoeringsbesluiten (art. 43).

Besloten mag worden dat de strafsancities op zich voldoende streng zijn om als afschrikkend beschouwd te worden. Veel zal daarbij echter ook afhangen van het vervolgingsbeleid van de Parketten terzake. Terecht wordt m.i. wel opgemerkt dat, nu geen enkele strafbepaling van de WVP ook maar iets preciseerd over het vereiste moreel of intentioneel element²⁰⁸, conform het gemeen recht, moet besloten worden dat algemeen opzet (*dolus generalis*)

²⁰⁷ Zie voor een bespreking van de sancties: M.-H. BOULANGER, C. DE TERWANGE en Th. LEONARD, *l.c.*, 387-388 en P. LEMMENS, *l.c.*, 441-442.

²⁰⁸ Art. 39, 5°, in fine, WVP hier buiten beschouwing gelaten.

dient aangetoond te worden om van een misdrijf te kunnen spreken.²⁰⁹ De loutere overtreding van een bepaling van de WVP lijkt dus geenszins voldoende. Dit zal wellicht onnodige bewijsmoeilijkheden met zich brengen voor het O.M., zodat de WVP dus ook op dit vlak zeker voor preciserende verbetering in aanmerking komt.

De Richtlijn zelf bevat geen sancties, maar verwijst hiervoor naar de lidstaten. Aan hen wordt opgedragen om passende maatregelen te nemen die de onverkorte toepassing van de bepalingen van de Richtlijn garanderen, en om sancties vast te stellen die zullen worden opgelegd in geval van inbreuk op de ter uitvoering van de Richtlijn vastgestelde bepalingen (art. 24).

VII. VERSCHILLEN DE PRIVACYWETTEN VAN ONZE BUURLANDEN VAN DE BELGISCHE WVP?

AFDELING 1. DUITSLAND

Duitsland was het eerste Europees land waar de bescherming van persoonsgegevens (Datenschutz) werd geregeld. Reeds op 27 januari 1977 werd de eerste Bundesdatenschutzgesetz tot stand gebracht. Een herziening van deze wet werd noodzakelijk door een arrest van het Bundesverfassungsgericht van 1983.²¹⁰ Dit arrest stelde immers het principe van de "informationelle Selbstbestimmung" voorop, m.a.w. het recht van elk individu om, binnen bepaalde grenzen, zelf te beslissen over het gebruik van persoonsgegevens die hem betreffen. Een wet van 1990 bouwde het principe van de "informationelle Selbstbestimmung" dan uiteindelijk in de Bundesdatengesetz in.²¹¹ Het principe van de nieuwe wet is immers zo dat de verwerking en het gebruik van persoonsgegevens verboden zijn tenzij de betrokkene zijn toestemming geeft (Datenschutz met Erlaubnisvorbehalt) of in die gevallen waarin een wet verwerking voorschrijft of toelaat. De bedoeling van de Datenschutzgesetz is dus veeleer het beschermen van een fundamenteel persoonlijkheidsrecht dan wel het louter bestrijden of vermijden van misbruiken bij de verwerking van persoonsgegevens.²¹² Het hoeft dan ook geen betoog dat de Duitse wet reeds wat de principes betreft veel verder gaat (en vooral veel meer privacybeschermend werkt) dan de Belgische. Terwijl in België verwerking van persoonsgegevens principieel toelaatbaar is tenzij uitdrukkelijk verboden of strijdig met het finaliteitsbeginsel²¹³, is in Duitsland

²⁰⁹ M.-H. BOULANGER, C. DE TERWANGE en Th. LEONARD, *l.c.*, 388.

²¹⁰ J. DUMORTIER, *Europese en Belgische reglementering over de behandeling van persoonsgegevens*, Leuven, ICRI, 1993, 9-10.

²¹¹ Voor een uitgebreide bespreking van die Wet, zie D. UNGNADE en Fr.-J. GORYNIA, "De BDSG-Novelle 1990: Auswirkungen auf die Kreditwirtschaft", *Zeitschrift für Wirtschafts- und Bankrecht* 1991, 121-127.

²¹² B.J. BOSWINKEL, "Het Bundesdatengesetz 1990", *T. Comp* 1993, I, 41-43.

²¹³ Cfr. *supra* nrs. 38 tot 50.

verwerking van persoonsgegevens principieel verboden tenzij uitdrukkelijk toegestaan door de betrokkene of door een wet. Terecht wordt er m.i. op gewezen dat men moet opletten voor een verabsolutering van het informatiele zelfbeschikkingsrecht²¹⁴; in een geïnternationaliseerde samenleving moeten gegevens weliswaar beschermd worden, maar toch ook vlot uitgewisseld kunnen worden. Men denke hierbij aan de vereisten van een vlot internationaal betalingsverkeer. Een evenwicht tussen het belang van de betrokkene en het algemeen (economisch) belang dient te worden gevonden. Bovendien moet ook rekening gehouden worden met de concurrentiepositie van de Duitse banken. Een veel strengere privacybescherming dan in de rest van Europa komt deze positie m.i. niet ten goede. Het vermijden van ongelijke concurrentieposities wat gegevensverwerking aangaat, is trouwens één van de oorzaken van het totstandkomen van een Privacyrichtlijn.

Een ander kenmerk van de Duitse wet is het onderscheid dat gemaakt wordt tussen de publieke en de private sector. Dit onderscheid komt o.m. duidelijk tot uiting in de wijze van beteugeling van overtredingen van het principe van de informatiele zelfbeschikking.²¹⁵ In de publieke sector werkt men met de rechtsfiguur van de "schadevergoeding zonder fout": niet toegelaten of onjuist gebruik van persoonsgegevens dat schade veroorzaakt, leidt tot schadevergoeding, ongeacht of er een fout voorhanden is. In de private sector werkt men met de omkering van de bewijslast ten voordele van de persoon wiens gegevens verwerkt worden. De houder van het bestand moet het bewijs van toestemming of wettelijke geoorloofdheid leveren. Door deze sanctioneringsmechanismen blijft het principe van de informatiele zelfbeschikking wellicht geen dode letter.

Het onderscheid tussen publieke en private sector is ook relevant voor de banksector.²¹⁶ Tot de publieke sector behoren in concreto o.m. de Deutsche Bundesbank, de DG-Bank en de kredietinstellingen van de zogenaamde "Bond mit Sonderaufgaben". Tot de private sector behoren de privé-kredietinstellingen en de vrije spaarkassen.

Een laatste typisch kenmerk van het Duitse systeem zijn de zogenaamde "Datenschutzbeauftragte".²¹⁷ In de private sector moet iedere onderneming met minstens vijf werknemers een verantwoordelijke voor de privacybescherming in de onderneming aanstellen. Deze krijgt dan het statuut van beschermd werknemer. Ook in de publieke sector worden, zowel op het niveau van de Länder als op het federaal niveau Datenschutzbeauftragte aangesteld. Deze instanties moeten toezien op de naleving van de regels en beschikken daartoe over een recht van toegang tot alle bestanden met persoonsgegevens.

²¹⁴ KI.-W. KNAUTH, "Datenschutz und grenzüberschreitender Datenverkehr in der Kreditwirtschaft", *Zeitschrift für Wirtschafts- und Bankrecht* 1990, 209-215.

²¹⁵ J. DUMORTIER, *o.c.*, 9.

²¹⁶ D. UNGNADE en Fr.-J. GORYNIA, *o.c.*, 124.

²¹⁷ J. DUMORTIER, *o.c.*, 9.

Aanmelding van verwerkingen van private ondernemingen aan de Datenschutzbeauftragte van de Länder of van het federaal niveau zijn slechts in beperkte gevallen vereist.²¹⁸

Ook het bankgeheim draagt bij tot de gegevensbescherming.²¹⁹ Volgens STEUER moet gegevensbescherming in de banksector trouwens beschouwd worden als het toepassen van het bankgeheim.²²⁰ Deze stelling gaat echter niet op voor de Belgische situatie.²²¹

B. FRANKRIJK

In Frankrijk is de verwerking van persoonsgegevens geregeld in de Wet "Informatique, fichiers et libertés" van 6 januari 1978. Centraal staat daar het principe van de "due process".²²² Art. 2 van de Franse wet verbiedt dat beslissingen over personen enkel en alleen worden genomen op grond van een verwerking die hun persoonsprofiel vastlegt.²²³ Het risico op foutieve beslissingen gesteund op onjuiste, verouderde of onvolledige gegevens is immers niet ondenkbaar. Meer algemeen gesteld, wordt eenieder het recht toegekend om de informatie en de redeneringen te kennen die worden gebruikt in geautomatiseerde gegevensverwerkingen waarvan de uitkomst hem of haar wordt tegengeworpen. Hierdoor wordt aan de privacy een nieuwe dimensie toegekend, namelijk de transparantie van de gegevensverwerking.²²⁴ De Franse wet erkent verder aan de persoon wiens gegevens verwerkt worden, in art. 26 het recht op verzet om deze gegevens aan derden door te spelen. In een contractuele relatie impliceert dit bv. dat geen gegevens mogen doorgegeven worden aan personen die er geen bestemming van zijn luidens het contract.²²⁵ De Franse wet voorziet ook een recht om te vergeten (*droit à l'oubli*). Dit recht is erop gericht om het bewaren van persoonsgegevens in de tijd te beperken. Niet meer actueel relevante informatie dient te worden gewist. Naar de banksector toe is de CNIL²²⁶ op dit vlak wel iets soepeler gebleken, dit om direct marketing mogelijk te maken.²²⁷ Bewaren van persoonsgegevens van iemand die een lening heeft lopen zou normaal, ingevolge "le droit à l'oubli", in de tijd beperkt moeten zijn tot de aflossing van die lening. Toch laat de CNIL, onder voorbehoud van verzet door de gewezen ontlenaar, blijvende bewaring voor marketingdoeleinden toe voor een periode van maximaal vijf

²¹⁸ De aangifteplicht is beperkt tot die ondernemingen die "Datenverarbeitung in Auftrag als Dienstleistung oder zur geschäftsmässigen Übermittlungsbetreiben" verrichten.

²¹⁹ M. SCHODEMEIER, "Le secret bancaire en République Fédérale de l'Allemagne", *Droit et Pratique du commerce international* 1990, 184-203.

²²⁰ S. STEUER, "Datenschutz in der EG", *Zeitschrift für Wirtschafts- und Bankrecht* 1992, 7.

²²¹ Cfr. supra sub nrs. 9 tot 12.

²²² J. DUMORTIER, *o.c.*, 11.

²²³ M.-H. BOULANGER, C. DE TERWANGE en Th. LEONARD, *l.c.*, 384.

²²⁴ F. KUITENBOUWER, "Losse einden van privacybescherming", *T. Comp* 1994/3, 92.

²²⁵ S. NERBONNE, *L'expérience française: l'application de la loi du 6 janvier 1978 au secteur bancaire*, Brussel, Studiedag Belgische Vereniging van Banken, 1993, 5.

²²⁶ CNIL: la Commission nationale de l'informatique et des libertés.

²²⁷ S. NERBONNE, *o.c.*, 5.

jaar na het aflopen van de lening. Verder erkent de Franse wet, net zoals de Belgische, een recht op informatie, een recht op toegang, het finaliteitsbeginsel, het verbod op verwerking van gevoelige gegevens. Het is dus duidelijk dat de Belgische wetgeving eens te meer zeer sterk geïnspireerd is op de Franse. Waarom dan niet de meer cruciale bepalingen (zoals het recht op verzet en het principe van due process), die tevens een groot privacybeschermend karakter hebben, werden overgenomen in de Belgische wet, blijft onduidelijk en strekt de Belgische wetgever zeker niet tot eer.

Geheel in overeenstemming met de centralistische Franse bestuurscultuur wordt het Franse systeem gekenmerkt door de oprichting van een centrale controle-autoriteit: de CNIL. De CNIL heeft een prestigieuze samenstelling: voorzitter is JACQUES FAUVET, gewezen hoofdredacteur van *Le Monde*. Verder bestaat ze uit parlementairen, leden van de sociaal economische raad, magistraten van de Raad van State en het Rekenhof en een aantal deskundigen.²²⁸ De Belgische CBPL is echter naar aloude Belgische gewoonte samengesteld op dubbel paritaire wijze: taalkundige pariteit en ideologische pariteit. Dit kan zorgen voor een probleem van niet algehele onafhankelijkheid. De CNIL daarentegen heeft een grote graad van onafhankelijkheid (o.m. ook t.o.v. de Franse regering) gekregen. Dit blijkt uit de vele garanties die in art. 8 van de wet werden ingebouwd.²²⁹ De belangrijkste bevoegdheden van de CNIL dienen onderscheiden te worden in een reglementerende bevoegdheid²³⁰ enerzijds en een krachtige onderzoeksbevoegdheid anderzijds.²³¹ Verder houdt de CNIL toezicht op de naleving van het recht om te vergeten (*droit à l'oubli*), het recht op toegang en de finaliteitsafwijking (*détournement de finalité*). Tenslotte heeft de CNIL ook waarschuwings- en sanctioneringsbevoegdheid en beschikt ze over de bekwaamheid om beroep te doen op het gerecht (*recours à la justice*).

Net zoals in Duitsland vindt men in de Franse Wet tevens een onderscheid tussen de private en de publieke sector.²³² In de publieke sector zijn verwerkingen van persoonsgegevens enkel mogelijk wanneer een wet of een reglement dit toelaat. Dergelijke regulering kan slechts tot stand komen na gemotiveerd advies van de CNIL. In de private sector moeten alle geautomatiseerde persoonsgegevensverwerkingen onderworpen worden aan een voorafgaande aangifte bij de CNIL.

Aangifte van alle verwerkingen bij de centrale controle-autoriteit CNIL bleek uitgesloten. Dit probleem werd opgelost door de zogenaamde "normes

²²⁸ J. DUMORTIER, "Privacybescherming en gegevensbescherming", *VJV* 1993/4, 12.

²²⁹ Voor een overzicht hiervan, zie bijdrage van de Voorzitter van de CNIL: FAUVET, J., "Informatique et vie privée", in X. (ed.), *Droit et informatique, Hermine et la puce*, Paris, Masson, 1992, 166.

²³⁰ Bijvoorbeeld het opstellen van normes simplifiées, cfr. infra.

²³¹ Zie daarover meer in J. FAUVET, "Informatique et vie privée", in X. (ed.), *o.c.*, 167-168.

²³² J. DUMORTIER, *o.c.*, 10.

simplifiées", uitgevaardigd door de CNIL. Deze heeft immers de wettelijke bevoegdheid om voor courante categorieën van verwerkingen, die bovendien kennelijk geen gevaar opleveren voor de persoonlijke levenssfeer, vereenvoudigde normen uit te vaardigen. Voor de banksector blijken vooral "norme simplifiée n° 12" i.v.m. rekeningbeheer²³³ en "norme simplifiée n° 13" i.v.m. kredietbeheer en leningen aan natuurlijke personen²³⁴ belangrijk. Deze "normes simplifiées" bevatten telkens een aantal algemene regels betreffende gebruik, finaliteit, toegang, beveiliging, bewaartermijn en mededeling van gegevens aan derden. Om een geautomatiseerde verwerking aan te vatten, volstaat een verklaring van de houder (bv. een bank) dat hij de vereenvoudigde normen zal naleven. In concreto betekent het systeem van de "normes simplifiées" voor de banksector dat voor bepaalde verwerkingen (bv. kredietbeheer, cliëntenbeheer) een eenvoudige verklaring bij de CNIL volstaat, terwijl voor andere verwerkingen (bv. credit scoring, direct marketing, prospectusbeheer,...) de gewone aangifteprocedure blijft bestaan.²³⁵

Besluitend kan men dus stellen dat de gelijkenissen tussen de Franse en Belgische wet treffend zijn. De Franse wet gaat echter op bepaalde cruciale punten verder dan de Belgische en werkt dan ook meer privacybeschermend. Franse en Belgische wet zijn bovendien kaderwetten. Voor beide dienden nog uitvoeringsmaatregelen te worden genomen. In Frankrijk gebeurde dit door de CNIL. In België is dit aan de gang via K.B.'s. De lasten van de actuele Franse wet en zijn uitvoeringsmaatregelen op de banksector lijken redelijk. Dit moet blijken uit volgende voorbeelden: strenge bewaartermijnen voorzien in de wet werden op grond van een belangenafweging onder welomschreven voorwaarden verlengd om *direct marketing* in de banksector mogelijk te maken. Anderzijds werd de grote administratieve last van de gewone aangifte bij de CNIL reeds aanzienlijk verlicht door het opstellen van *normes simplifiées* voor enkele courante verwerkingen in de financiële sector. Als deze tendens zich verder voortzet, zullen deze *normes simplifiées* eerder regel dan uitzondering worden.

C. VERENIGD KONINKRIJK

In het Verenigd Koninkrijk werd de bescherming van persoonsgegevens tot stand gebracht door Data Protection Act van 12 juli 1984. De wet roept een Data Protection Registrar en een Data Protection Tribunal in het leven.²³⁶ Bij de Registrar moeten alle houders van persoonsgegevens zich laten

²³³ Norme simplifiée n° 12, concernant les traitements automatisés d'informations nominatives relatifs à la tenue des comptes de la clientèle et le traitement des informations d'y rattachant par les établissements bancaires et assimilés, *J.O.*, 19 augustus 1980.

²³⁴ Norme simplifiée n° 13, concernant les traitements automatisés d'informations nominatives relatifs à la gestion des crédits ou des prêts consentis à des personnes physiques par les établissements de crédit, *J.O.*, 19 augustus 1980.

²³⁵ S. NERBONNE, *o.c.*, 3-4.

²³⁶ J. DUMORTIER, *Europese en Belgische reglementering over de behandeling van persoonsgegevens*, Leuven, ICRI, 1993, 11.

registreren.²³⁷ Een dergelijke registratie is slechts 3 jaar geldig: dan moet ze hernieuwd worden. Zolang men echter niet geregistreerd is, mag men in principe geen geautomatiseerde verwerking van persoonsgegevens verrichten. Er zijn uitzonderingen (o.m. voor zogenaamde "home users") voorzien; uiteraard vallen de financiële instellingen daar niet onder. Bij de registratie kan de Registrar aan de houder van het bestand (de "data user") richtlijnen ("notices") opleggen. Tegen dergelijke beschikkingen van de Registrar is beroep bij de Data Protection Tribunal mogelijk.²³⁸

Ook in de Data Protection Act staat het finaliteitsbeginsel centraal. Bij de registratie moet men de finaliteit(en) aangeven waarvoor men wil registreren. Om de registratie vlot te laten verlopen, werd door de Registrar een "purpose Code" met 70 veel voorkomende finaliteiten opgesteld.²³⁹ Voor de banksector lijken de voornaamste finaliteiten die in de purpose Code werden opgenomen, de volgende te zijn: personeelsadministratie, marketing, cliëntenadministratie, kredietadministratie, financiële diensten en verzekeringen. Bij de aangifte hoeft men slechts één of meer finaliteiten aan te kruisen. Dit systeem van de purpose Code komt in grote lijnen overeen met de Franse "normes simplifiées" en het Belgische "lexicon". In al deze landen werd blijkbaar de nood aan een administratieve versoepeling ingezien.

Op 6 december 1990 heeft het Brits bankwezen een ontwerp gedragscode voor het betalingsverkeer opgesteld. Hoewel deze ontwerpcode het ruimere veld van de relatie bank-consument in het kader van het particuliere betaalverkeer behandelt, komt ook de vertrouwelijkheid en de bescherming van de persoonsgegevens van de cliënten hierin aan bod.²⁴⁰ Het ontwerp werd opgesteld door British Bankers' Association (BBA)²⁴¹, de Building Societies Association (BSA) en de Association for Payment and Clearing Services (APACS). Met deze ontwerp-code wilde het Britse bankwezen reageren op het Jack Report.²⁴²

In juli 1994 werden dan, middels een aantal amendementen, additionele strafbepalingen toegevoegd aan de Criminal Justice and Public Order Bill, met effect op Section 5 van de Data Protection Act.²⁴³ Zo was het reeds verboden om persoonsgegevens door te geven aan niet gemachtigde (unauthorised) personen. Op basis van de nieuwe wetgeving begaat nu ook een misdrijf hij die

²³⁷ Voor alle informatie i.v.m. samenstelling, middelen en activiteiten van de Britse Data Protection Registrar, zie J. DUMORTIER, "Privacybescherming en gegevensverwerking", *VJJ* 1993/4, 12-14.

²³⁸ J. DUMORTIER, *o.c.*, 11.

²³⁹ J. DUMORTIER, *o.c.*, 11.

²⁴⁰ J. BERKVEN, "Draft Code on banking practice", *T. Comp.* 1991/3, 98-99.

²⁴¹ De tegenhanger van de Belgische Vereniging van Banken.

²⁴² X., "Het Jack Report", *T. Comp.* 1989/4, 158; Ch. CLIFFORD, *Banking & Investment Services*, London, IFR Publishing Limited, 1989, 103-105.

²⁴³ ROWE, "The Data Protection Act 1984: does it have any shortcomings?", *Computer & Telecoms Law Review* 1994/4, 64-65.

als niet gemachtigd (unauthorised) persoon de ontsluiting van persoonsgegevens nastreeft. Voor het misdrijf is zelfs geen misleiding vereist; het loutere nastreven (to proceed) is al voldoende. De Britse banksector was uiteraard opgezet met deze nieuwe wet. Wie voortaan met valse identiteitspapieren persoonsgegevens van iemand anders bij de bank tracht te verkrijgen, begaat een misdrijf en zal nu wel twee keer nadenken. Op die wijze vermindert voor de bank het risico dat ze de vertrouwelijkheid van de persoonsgegevens van haar cliënten (ongewild) schendt. Een tweede amendement creëerde een misdrijf voor hij die vertrouwelijke financiële informatie verkoopt aan een derde wetende dat deze informatie oneerlijk of via misleiding verkregen werd. Hoewel deze misdrijven tevens aspecten van de discretieplicht bevatten, zijn ze m.i. toch relevant voor de bescherming van persoonsgegevens in Groot-Brittannië.

D. NEDERLAND

In Nederland wordt de informationele privacy beschermd door de Wet van 28 december 1988 houdende regels ter bescherming van de persoonlijke levenssfeer in verband met persoonsregistraties (hierna: Wet Persoonsregistraties).²⁴⁴ Terwijl de Belgische wet toepasselijk is op "verwerkingen", is de Nederlandse wet van toepassing op registraties.

Een persoonsregistratie is in art. 1 van de Wet Persoonsregistraties gedefinieerd als een samenhangende verzameling van op verschillende personen betrekking hebbende persoonsgegevens die langs geautomatiseerde weg wordt gevoerd of met het oog op een doeltreffende raadpleging van die gegevens systematisch is aangelegd. Daarbij is niet van belang of de verzameling ook effectief wordt gebruikt, noch of de verzameling op één fysieke locatie aanwezig is.²⁴⁵ Cruciaal in de bovenstaande definitie is wat bedoeld wordt met een persoonsgegeven. Conform de toelichting bij de Wet moeten als persoonsgegevens worden beschouwd alle gegevens die omtrent een bepaalde persoon informatie kunnen verschaffen.²⁴⁶

De kernbepaling van de Wet Persoonsregistraties is art. 4: "een persoonsregistratie mag slechts worden aangelegd voor een bepaald doel, waartoe het belang van de houder redelijkerwijze aanleiding geeft". Een persoonsregistratie mag slechts persoonsgegevens bevatten die rechtmatig zijn verkregen en in overeenstemming zijn met het doel waarvoor de registratie is aangelegd (art. 5). De opgenomen persoonsgegevens mogen bovendien slechts gebruikt worden voor doeleinden die met het doel van de persoonsregistratie verenigbaar zijn (art. 6).²⁴⁷

²⁴⁴ Wet houdende regels ter bescherming van de persoonlijke levenssfeer in verband met persoonsregistraties, *Stbl.*, 1988, 665.

²⁴⁵ V.A. VAN DE POUS, "Wet persoonsregistraties", in X. (ed.), *Beheer van Data-base systemen*, Deventer, Kluwer, 1994, 6.

²⁴⁶ V.A. VAN DE POUS, *l.c.*, 5.

²⁴⁷ J. DUMORTIER, *Europese en Belgische reglementering over de behandeling van persoons-*

De opname in een bestand van gevoelige gegevens (zoals godsdienst, politieke gezindheid, enz.) wordt in Nederland, net zoals in België, aan sterke beperkingen onderworpen.²⁴⁸ In Nederland gebeurt deze beperking echter niet in de wet zelf, maar in een afzonderlijke algemene maatregel van bestuur.²⁴⁹ De verwerking van gevoelige gegevens wordt slechts toegelaten met schriftelijke toestemming van de betrokkene of "indien de verwerking noodzakelijk is met het oog op de gewichtige belangen van de houder en de persoonlijke levenssfeer van de betrokkene daardoor niet onevenredig wordt geschaad". De afweging tussen de belangen van de houder en de persoonlijke levenssfeer van de betrokkene is kenmerkend voor de Nederlandse Wet.²⁵⁰

Mededeling aan derden van persoonsgegevens is, in tegenstelling met de Belgische WVP, principieel verboden. Mededeling aan derden is enkel toelaatbaar als dit voortvloeit uit het doel van de registratie, wanneer een wettelijk voorschrift dit vereist of wanneer de geregistreerde hiertoe de toestemming geeft (zie art. 11 Wet Persoonsregistraties).²⁵¹

De Nederlandse Wet Persoonsregistraties bevat daarnaast een aantal bepalingen zoals i.v.m. de rechten van de betrokkene, de aanmelding en de kennisgeving, die vrijwel identiek zijn aan de Belgische bepalingen van de WVP terzake.

In de Nederlandse wetgeving wordt verder sterk de nadruk gelegd op zelfregulering (art. 15 Wet persoonsregistraties). Voor sectoren houdt dit de mogelijkheid in om gedragscodes op te stellen. De organisatie die een dergelijke code opstelt, moet representatief zijn voor de betrokken sector. Bovendien moet er tegenspraak ("gelegenheid tot opmerkingen en bezwaren") geweest zijn binnen de sector. Aan de Registratiekamer²⁵² kan gevraagd worden om de voorgestelde gedragscode in overeenstemming met de wet te verklaren. Een dergelijke verklaring is echter niet bindend voor hoven en rechtbanken. Daarenboven geldt ze slechts voor een periode van vijf jaar. Het systeem van de gedragscodes beoogde meer soepelheid in de Wet in te bouwen. In de praktijk bleek het uitwerken van dergelijke codes in de meeste sectoren, waaronder de banksector, een langdurige en bureaucratische procedure.²⁵³ Voor de banksector werd een privacy-gedragscode aangenomen door de Registratiekamer op 29 maart 1989.²⁵⁴ Het weze duidelijk dat een

gegevens, Leuven, ICRI, 1993, 13; V.A. VAN DE POUS, *l.c.*, 8-9.

²⁴⁸ J. HOLVAST, "Wet persoonsregistraties: een wet die (nog) niet leeft bij de registratiehouders", *Informatie* 1993, 698.

²⁴⁹ Besluit gevoelige gegevens, *Stbl*, 1993, nr. 158.

²⁵⁰ J. DUMORTIER, *o.c.*, 13.

²⁵¹ X., "De Wet persoonsregistraties en de gedragscode voor het bankwezen", *De Spaarbank* 1989, 105.

²⁵² Dit is de Nederlandse tegenhanger van de Belgische CBPL en de Franse CNIL

²⁵³ J. DUMORTIER, *o.c.*, 13.

²⁵⁴ E. MEYSMANS, "Bancaire bestanden en privacy-bescherming in België", *T. Comp.* 1992/1, 13.

dergelijke code slechts een aanvulling op de Wet uitmaakt.²⁵⁵

Dat een sectorale gedragscode in het bijzonder voor de banksector een aantal voordelen kan bieden, moge blijken uit de volgende voorbeelden uit de Nederlandse Gedragscode voor het Bankwezen. In de code gaat men voor de banksector uit van één enkele cliënt-registratie, gegrond op een totale visie op de cliënteel.²⁵⁶ Een dergelijke totale visie is in de huidige stand van de Belgische wetgeving niet denkbaar, hoewel aanlokkelijk voor de Belgische banksector.²⁵⁷ Verder wordt in de Nederlandse gedragscode voor het bankwezen ook bepaald dat het verstrekken van gegevens interbancair of aan de Bankgirocentrale in het kader van het betalingsverkeer niet kan worden gekwalificeerd als het verstrekken van gegevens aan derden. Het beschikbaar stellen van cliëntgegevens aan verzekeraars, touroperators of Eurocard, alsook de loutere uitwisseling van cliëntgegevens interbancair wordt daarentegen wel als een verstrekking van gegevens aan derden beschouwd.²⁵⁸

E. BESLUIT BIJ HET RECHTSVERGELIJKEND OVERZICHT

Uit dit beknopt rechtsvergelijkend overzicht blijkt duidelijk dat er in de diverse Europese landen verschillende klemtonen gelegd werden bij de aanpak van de bescherming van persoonsgegevens. Staat in Duitsland het informationele zelfbeschikkingsrecht voorop, dan wordt in Frankrijk weer eerder de nadruk gelegd op het beginsel van due process. In Nederland en Engeland biedt de wetgeving dan weer eerder een kader dat via zelfregulering (gedragscodes) sectoraal aangepast en versoepeld kan worden. Naast de verschillende klemtonen in de diverse wetgevingen, zijn toch ook enkele gelijkenissen waar te nemen. Het concept van de doelgebondenheid (het finaliteitsbeginsel) staat overal centraal.

Het is zeer moeilijk en ook te delicaat om een waarde-oordeel te uiten ten voordele van deze of gene wetgeving. In bovenstaande werd eerder getracht telkens de bijzondere kwaliteiten van elke wetgeving naar voor te brengen. Wat wellicht wel geconcludeerd mag worden, is dat de Belgische WVP, vergeleken bij de buitenlandse wetgeving, zeer mager uitvalt. Het ontbeert de Belgische wetgeving vooral aan een nijpend gebrek aan visie.²⁵⁹

²⁵⁵ M.A. BERKVENS, "De privacy-code voor het bankwezen", *Bank- en effectenbedrijf* 1989/20, 21.

²⁵⁶ X., "De Wet Persoonsregistraties en het smalle pad tussen efficiëntie en bankwezen", *De Spaarbank*, 1989, 110.

²⁵⁷ Cfr. supra sub nrs. 20 tot 22 voor argumentatie.

²⁵⁸ X., "De Wet persoonsregistraties en de gedragscode voor het bankwezen", *De Spaarbank* 1989, 110; M.A. BERKVENS, "De privacy-gedragscode voor het bankwezen", *Bank- en effectenbedrijf* 1989, 20-25; B.B. VAN DEN BERGH, "De bancaire codes in Nederland", *De Spaarbanken*, 1992, 44-52.

²⁵⁹ Cfr. infra: zie algemeen besluit.

Het grootste probleem dat echter voortvloeit uit dit rechtsvergelijkend deel is precies de verscheidenheid zelf op inhoudelijk, maar vooral op praktisch-organisatorisch vlak tussen de diverse wetgevingen. Door de internationalisering van de economie in het algemeen en de financiële sector in het bijzonder, dient gegevensbescherming niet meer zozeer nationaal, maar des te meer internationaal te worden aangepakt. Daarbij moet bovendien rekening gehouden worden met de steile opgang van onderling verbonden databanken en netwerken die overal ter wereld geconsulteerd kunnen worden. Een ander argument pro de internationale aanpak van gegevensbescherming is gelegen in de concurrentievervalsing die kan voortvloeien uit separate nationale wetgevingen inzake privacy. Aangezien informatie een commercieel goed is, betekent een rigidere nationale regulering een nadeel in de concurrentiepositie t.o.v. die landen met een minder strenge privacyregulering.

Omdat harmonisering de beste garantie biedt voor een adequate gegevensbescherming enerzijds en een gelijke concurrentiepositie anderzijds, heeft men op het vlak van de Europese Unie, waarvan de lidstaten sterk economisch op elkaar gericht zijn, terecht besloten tot een eenmaking van de persoonsgegevensbescherming via de techniek van de Richtlijn. Daarbij is men bovendien zo verstandig geweest om de kwaliteiten van de diverse nationale wetgevingen samen te smelten tot een geheel dat bovendien een werkbaar instrument lijkt te worden. De bepalingen van de vastgestelde tekst van de Richtlijn werden hierboven reeds toegelicht in Hoofdstuk III, IV, V en VI, waar ze telkens tegenover de corresponderende bepalingen van de WVP werden geplaatst.

Tenslotte moet hier ook gewezen worden op het belang van de Conventie nr. 108 van de Raad van Europa. Dit instrument bevat o.m. bepalingen die het internationaal gegevensverkeer met een aantal landen die (nog) geen lid zijn van de Europese Unie, maar wel van de Raad van Europa, enerzijds beschermen en anderzijds van belemmeringen ontdoen.

VIII. ALGEMEEN BESLUIT

Het besluit heeft niet de bedoeling de detailkritieken en de partiële conclusies die in de loop van dit werk werden geformuleerd, te herhalen. Na een algemene beoordeling van de huidige WVP zal getracht worden tot een conclusie te komen over hoe het nu verder moet met de persoonsgegevensbescherming in België.

Dat de huidige privacyregulering als ongelukkig moet bestempeld worden, staat als een paal boven water. Allereerst ontbreken een aantal cruciale privacybeschermende regels in de huidige wet. Hoe kan men nu immers spreken van een degelijke privacybescherming als er nergens ook maar enig

recht op verzet, zoals in het Duitse recht, is ingebouwd in de wet.²⁶⁰ Niemand kan zich immers verzetten tegen de verwerking van zijn persoonsgegevens.²⁶¹ Men heeft enkel het recht om geïnformeerd te worden over een dergelijke verwerking, benevens enkele, blijkens de praktijk, mineure rechten zoals het recht op toegang en het recht op verbetering. Bovendien besteedt de wet nauwelijks of geen aandacht aan de termijn van bewaring van gegevens in een bestand. Het "droit à l'oubli" van het Franse recht vindt geen weerklank in het Belgische recht. Tenslotte worden ook nauwelijks beperkingen gesteld aan het meedelen aan derden van persoonsgegevens uit een bestand. Ook hier vormt slechts een administratieve verplichting, met name de kennisgeving door wie die verkregen gegevens verwerkt, het enige beletsel. Gelukkig is er op dit punt, voor wat de financiële sector althans betreft, nog de discretieplicht die de privacy van de persoon wiens gegevens verwerkt worden, goeddeels garandeert.

Wat in de wet vervolgens wel grondig uitgewerkt werd, zijn de talrijke administratieve verplichtingen die aan de houders van een bestand worden opgelegd. Men denke hier aan de staat die dient te worden opgemaakt en de voorafgaande aangifte bij de CBPL. Daarenboven wordt aan de houders per verwerking nog eens een belasting geheven. Wil de overheid de investering in automatisering hiermee afremmen?

Tenslotte moet ook het gebrek aan visie van de wetgever en de besluitgever aan de kaak gesteld worden. Eerst maakt men een wet met onwerkbaar concepten waarvan men bovendien de gevolgen niet weet te overzien. Vervolgens stelt de regering overhaast en, inhoudelijk, tegen de adviezen van de deskundigen van de CBPL in, Koninklijke Besluiten vast ten einde tot een reële privacybescherming te komen. Na zware, doch terechte kritiek van bepaalde sectoren, waaronder de banksector, op sommige van deze zo mogelijk nog onzinnigere regels (bv. K.B. nr. 9 i.v.m. collectieve kennisgeving), besluit de regering deze K.B.'s, nog voor hun inwerkingtreding, op te schorten. Intussen kwamen reeds wijzigende K.B.'s tot stand (bv. K.B. nr. 9 gewijzigd door K.B. nr. 15; K.B. nr. 12 gewijzigd door K.B. nr. 12 bis).

Wat biedt de toekomst? In kringen van de CBPL kon vernomen worden dat men eerst, in overleg met de betrokken sectoren, tot een werkzame wet wil komen, middels een aantal Koninklijke Besluiten die ons intussen bereikten en binnenkort zullen bereiken. Vervolgens zou men dan werk gaan maken van de implementatie van de Richtlijn in de Belgische rechtsorde.

M.i. mag betwijfeld worden of dit wel de juiste werkwijze is. Gevreesd mag worden dat de WVP, met zijn conceptuele beperktheden, wel nooit een goed werkinstrument zal worden, zelfs niet met verregaande

²⁶⁰ Cfr. supra.

²⁶¹ Uitzondering moet hier gemaakt worden voor wat betreft de gevoelige gegevens.

uitvoeringsmaatregelen. Bovendien verloopt het onderhandelen van die K.B.'s met de betrokken sectoren stroef. Hierdoor gaat kostbare tijd verloren voor de privacybescherming. Men weet immers dat men het werk opnieuw zal moeten beginnen eens dat de Richtlijn geïmplementeerd is. Implementatie van die Richtlijn zal trouwens grondige wijzigingen aan de WVP zelf noodzakelijk maken.

Zou men dan ook niet beter meteen de WVP zo snel mogelijk conformeren aan de Richtlijn en pas dan de nog noodzakelijke uitvoeringsmaatregelen vaststellen? Dit lijkt mij althans, mede vanuit rechtseconomisch oogpunt, de beste oplossing te zijn. Bovendien zou men dan, wat de uitvoeringsmaatregelen betreft, een sectorale benadering kunnen toepassen. Dit zou dan kunnen leiden tot een realistische en tevens adequate bescherming van persoonsgegevens in alle sectoren. Misschien kan daarbij het Nederlandse voorbeeld van de zelfregulering in bepaalde sectoren gevolgd worden. Een dergelijke adequate bescherming zou bovendien moeten gepaard gaan met een minimale administratieve belasting voor de houders. Deze administratieve lasten zijn immers slechts de transactiekosten van de privacywet en mogen dus geenszins een doel op zich vormen.²⁶²

²⁶² Stof bijgehouden tot 1 november 1996.