'Protecting privacy in this rapidly transforming online landscape demands agile, creative and effective responses.'

J. Stoddart[1]

[1] J. STODDART, 'Privacy in the Era of Social Networking: Legal Obligations of Social Media Sites', *Sask. L. Rev.* 2011, 263.

VOORWOORD

De relatie tussen de technologische ontwikkelingen in de informatiemaatschappij en het recht is een zeer interessant onderzoeksdomein. De laatste jaren is er veel te doen geweest over de bescherming van privacy op sociale netwerksites. Sociale netwerksites zijn een belangrijk deel gaan uitmaken van het dagelijkse leven. Het zijn vooral minderjarigen die vele uren spenderen op deze online platformen, maar zich niet of nauwelijks bewust zijn van de gevolgen voor hun persoonlijke levenssfeer. In dit werkstuk worden de privacygevoelige aspecten van minderjarigen op sociale netwerksites als leidraad genomen voor een zoektocht naar de meest geschikte wijze van regulering. Deze masterproef gaat dieper in op het nieuwe voorstel tot verordening van 25 januari 2012 dat het bestaande Europees wettelijk kader van gegevensbescherming zal vervangen. De wijzigende en nieuwe bepalingen gericht op kinderen en sociale netwerkdiensten worden geanalyseerd en geëvalueerd om het nieuwe instrument tegenover de in dit domein bestaande vormen van alternatieve regulering te plaatsen.

Graag wil ik een aantal mensen bedanken die betrokken zijn geweest bij de totstandkoming van deze masterproef. In de eerste plaats wens ik mijn promotor Prof. Dr. Peggy Valcke te bedanken voor de deskundige begeleiding gedurende het schrijfproces. Tevens wil ik Eva Lievens, onderzoekster bij het ICRI, bedanken voor de handige tips en feedback. Mijn dankwoord gaat mede uit naar het 'Europe Direct Contact Centre' dat mij nuttige informatie heeft verschaft omtrent het nieuwe voorstel tot verordening en de relevante beleidsdocumenten. Ten slotte ben ik dank verschuldigd aan mijn ouders, vriendin en vrienden voor de steun gedurende deze opleiding en niet in het minst gedurende de tijd die werd besteed aan dit werkstuk.

INHOUDSTAFEL

INLEIDING

Situering en probleemstelling

1. Het internet heeft zich ontwikkeld tot hét onmisbare informatiemedium in het digitale tijdperk. Sociale netwerksites (afgekort: SNS) zoals Facebook en Twitter, waarop iedereen persoonlijke informatie kan plaatsen en foto's, video's, muziek en internetlinks kan delen, zijn niet meer weg te slaan uit het dagelijkse leven van een minderjarige. Uit een studie van 'EU Kids Online' in opdracht van de Europese Commissie blijkt dat 77% van kinderen in de EU tussen dertien en zestien jaar en 38% van kinderen tussen negen en twaalf jaar een profiel hebben aangemaakt op een SNS. 26% van die gebruikers hebben een publiek profiel. 15% van de kinderen tussen negen en twaalf jaar hebben meer dan 100 'vrienden' op hun profiel.[2] Het aantal SNS-gebruikers en -aanbieders blijft bovendien exponentieel toenemen.

2. Deze nieuwe sociale mediaplatformen bieden ongetwijfeld voordelen[3], maar de ongebreidelde online informatiestroom brengt ernstige gevaren met zich mee voor minderjarige internauten.[4] Naast risico's zoals het blootstellen van

---

[2] 'Risks and safety on the internet: The perspective of European children. Full findings and policy implications from the *EU Kids Online* survey of 9-16 year olds and their parents in 25 countries', 13 januari 2011. Te raadplegen op: http://www2.cnrs.fr/sites/en/fichier/rapport_english.pdf.

[3] Zo geeft het Europees Economisch en Sociaal Comité in een advies van 2009 de volgende positieve aspecten van SNS aan: (1) de garantie en de uitoefening van het recht op vrije meningsuiting in een bepaalde sociale en politieke context, (2) het ontstaan en de vorming van onlinegemeenschappen, (3) (vernieuwd) contact met familie en vrienden en de mogelijkheid om onderling te communiceren, (4) het voorkomen van risicosituaties voor minderjarigen die via SNS hulp kunnen inroepen en (4) reclame voor goederen en diensten en een stijging van de elektronische handel. Zie: Europees Economisch en Sociaal Comité, Advies over de impact van sociale netwerksites op burgers/consumenten, 4 november 2009, 4. Te raadplegen op: https://toad.eesc.europa.eu/ ViewDoc.aspx?doc...2009_AC_NL.

[4] Enkele voorbeelden kunnen deze cybergevaren illustreren. Begin dit jaar pleegde een Australisch meisje zelfmoord na het slachtoffer te zijn geweest van cyberpesten op Facebook. ('Tiener stapt uit leven na pesterijen op Facebook', *DS* 12 januari 2012) Wanneer een kind op school wordt gepest, kent men meestal de dader en kan derhalve op tijd worden opgetreden. Pesten via het internet, zoals het hacken van emailaccounts, bedreigingen of het plaatsen van vervelende foto's, kan veel indringender zijn voor het slachtoffer. Cyberpesters kunnen niet altijd geïdentificeerd worden omwille van de anonimiteit en/of identiteitsvervalsing. Bovendien kunnen cyberpesters 24 uur op 24 uur actief zijn en zijn ze zich niet of minder bewust van de impact op het slachtoffer. Zie ook: 'Risks and safety on the internet. The perspective of European children. Full Findings and policy implications from the EU Kids Online Survey of 9-16 year olds and their parents in 25 countries', 13 januari 2011, 61-65. Een ex-vriendje die naaktfoto's had verspreid van zijn ex-vriendin op Facebook uit wraak na een afgelopen relatie is een ander zorgbarend voorbeeld. Kortgeleden pakten het Nieuwsblad en het Laatste Nieuws uit met foto's van de overleden kinderen van het busongeval in Zwitserland die ze zonder toestemming van de ouders op de voorpagina's hadden geplaatst. ('Lieten: foto's van slachtoffers busongeval publiceren is er ver over', *Knack* 16 maart 2012. Te raadplegen op: http://www.knack.be/nieuws/ belgie/lieten-foto-s-van-slachtoffers-busongeval-publiceren-is-er-ver-over/article-40000682181 28.htm) Deze foto's werden ongetwijfeld van het internet geplukt. Profielen van minderjarigen kunnen immers moeiteloos worden opgezocht via externe zoekrobots. Dit betekent dat deze ook beschikbaar zijn voor potentiële seksuele delinquenten en de deur open laten voor 'online grooming'. Een 'online groomer' is iemand die online contact met een kind maakt met de bedoeling een seksuele relatie te ontwikkelen waarbij o.a. aan 'cyberseks' of seks d.m.v. lichamelijk contact wordt gedaan. (Zie: Europese Commissie, 'Online Abuse: Literature Review and Policy Context' (in het kader van het

kinderen aan schadelijke en ongepaste inhoud[5] kan de ongecontroleerde verspreiding en toegang van informatie op wereldschaal gemakkelijk een verlies van zeggenschap van het individu over de gegevens die hij of zij online meedeelt, teweegbrengen.[6] Uit een onderzoek in 2005 aan de Universiteit van Antwerpen waarbij 294 websites, die zich hoofdzakelijk richtten naar minderjarigen, werden geanalyseerd, bleek dat toen al acht op de tien websites op één of andere manier persoonsgegevens verzamelden van minderjarigen. Van die websites voorzag 40% een privacy statement. Slechts 12% van de statements vermeldden iets van informatie over privacy voor ouders en/of kinderen.[7] We zijn ondertussen bijna tien jaar verder en tegenwoordig circuleren onmetelijke hoeveelheden persoonlijke gegevens van minderjarigen op sociale netwerkplatformen. Het feit dat deze content 'voor altijd' op de servers van de SNS-aanbieders blijft staan doet ernstige vragen rijzen over de bescherming van de privacy. Daarenboven heeft het grote aantal SNS-gebruikers een enorme impact op het privéleven van niet-gebruikers wanneer gegevens van deze laatsten op een SNS wordt geplaatst.[8] In een sociale netwerkomgeving is in feite niets anoniem en laat men hoe dan ook een digitale voetafdruk achter. Zo kunnen adverteerders deze persoonsgegevens opvissen en gebruiken om reclame te maken.[9]

3. Het internet houdt niet alleen risico's in voor het privéleven van minderjarigen. Volwassenen kunnen evenzeer het slachtoffer worden van een miskenning van hun privacy wanneer informatie op SNS gebruikt wordt voor

---

Europese Online Grooming Project), februari 2011, 8. Te raadplegen op: http://www.europeanonlinegroomingproject.com/wp-content/file-uploads/EOGP-Literature-Review.pdf). Zowel binnen het kader van de EU als de Raad van Europa werden tal van initiatieven genomen ter bestrijding van 'online grooming'. Zo werd op het niveau van de Raad van Europa het Verdrag inzake de bescherming van kinderen tegen seksuele uitbuiting en seksueel misbruik gesloten op 13 juli 2007. Artikel 23 verplicht de verdragsstaten om 'grooming' strafrechtelijk te beteugelen. De EU vaardigde in 2004 o.a. het kaderbesluit 2004/68/JBZ ter bestrijding van seksuele uitbuiting van kinderen en kinderpornografie uit. In een aanbeveling van het Europese Parlement van 3 februari 2009 wordt de ondertekening, ratificatie en implementatie van het Verdrag van de Raad van Europa en de uitvoering van het kaderbesluit aangemoedigd.

[5] Illegale inhoud zoals kinderpornografie dat strafrechtelijk wordt beteugeld dient men te onderscheiden van andere schadelijke inhoud dat aanstootgevend kan zijn voor minderjarigen, maar daarom nog niet illegaal is en perfect toegankelijk is voor volwassen zoals pornografie of nodeloos geweld. Zie: E. LIEVENS en J. DUMORTIER, 'Bescherming van minderjarigen online: stand van zaken en blik op de toekomst', *Computerr.* 2005/2, 60. (Hierna: E. LIEVENS e.a., 'Bescherming minderjarigen online')

[6] Commissie voor de bescherming van de persoonlijke levenssfeer, Advies 38/2002 betreffende de bescherming van de persoonlijke levenssfeer van minderjarigen op internet, 16 september 2002. Te raadplegen op: http://www.internet-observatory.be/internet_observatory/pdf/_advice_privacy_nl.pdf.

[7] 'Cyberkids' e-Privacy. Minderjarigen, minder rechten? (Privacy Paper Nr. 4)', Universiteit Antwerpen (Department of Communication Studies), 2005, 6. Te raadplegen op: http://www.e-privacy.be/PrivacyPaper4-Cyberkids-e-Privacy.pdf. (Hierna: Privacy Paper Cyberkids)

[8] P. VAN EECKE en M. TRUYENS, 'Privacy en sociale netwerken', *Computerr.* 2010/3, 127. (Hierna: P. VAN EECKE en M. TRUYENS, 'Privacy en sociale netwerken')

[9] 'Beperk uw digitale voetafdruk', nieuwsbrief Test-Aankoop, maart 2010. Te raadplegen op: http://mcs.testaankoop.be/default.aspx?show=1351&src=645203&lge_id_c=N&prm_id_c=TANLSG&cop_id_c=N1004.01.

oneigenlijke doeleinden.[10] Potentiële schade beperken bij online informatie-uitwisseling begint dan ook in de eerste plaats bij de gebruiker zelf: 'bezint eer ge begint'. Kinderen en jongeren zijn zich evenwel minder bewust dan volwassenen van de gevaren voor hun persoonlijke levenssfeer op het internet. Bovendien hebben zij in de meeste gevallen betere technische 'skills' verworven dan hun ouders of leerkrachten en ontwikkelt deze generatiekloof zich niet evenredig met het bewustzijn om op een verantwoordelijke en omzichtige wijze om te springen met het aanzienlijk aanbod aan online informatie.[11] Uit de 'Social Mediabarometer' van WDM Belgium blijkt dat een zeer groot gedeelte van de jonge SNS-gebruikers niet op de hoogte is van de maatregelen die sociale netwerken nemen om de privacy beter te beschermen.[12] Kinderen en jongeren vormen aldus een bijzondere risicogroep en hebben des te meer baat bij adequate veiligheidsmaatregelen en richtsnoeren die hun privacy op SNS beogen te beschermen.

4. In het licht van de razendsnel ontwikkelende technologieën en online informatiediensten is het uitvaardigen van passende en efficiënte regelgeving geen sinecure. Rechtsregels ter bescherming van minderjarigen uit het traditionele mediarecht gericht op kranten, radio- en televisieomroepen, kabeldistributie, telecommunicatie, audiovisuele media en andere massacommunicatiemiddelen vallen niet zomaar te transponeren op nieuwe vormen van sociale media in de huidige informatiemaatschappij. Bovendien dienen wetgevers rekening te houden met alle relevante stakeholders in een sociale netwerkomgeving.[13] Niet alleen de aanbieders van sociale netwerkdiensten, maar tevens de jonge gebruiker zelf en derde partijen zoals websitehouders en aanbieders van applicaties zijn betrokken in het complexe juridische spectrum van SNS. Belangrijk is dan ook na te gaan welke afdwingbare plichten er bestaan of kunnen bestaan in hoofd van deze spelers om minderjarigen de hoogste graad van privacybescherming te kunnen verzekeren conform Europese en nationale wetgeving.

De complexe online realiteit maakt het dus moeilijk voor wetgevers om hard law-bepalingen ter zake uit te vaardigen. Dit is ook de reden waarom tot op vandaag geen specifieke wetgeving betreffende SNS voorhanden is. Jammer genoeg is er

[10] Zo kan een werkgever een profiel raadplegen ter controle van zijn werknemers of worden nepprofielen aangemaakt om te spioneren bij een ander bedrijf. Tevens kan om het even wie vervelende foto's plaatsen van iemand op een SNS zonder dat die persoon daar zelf op de hoogte van is. In september vorig jaar veroordeelde de Gentse correctionele rechtbank een vrouw uit Kortemark tot zeven maanden celstraf met uitstel. De vrouw had een vals Facebook-profiel aangemaakt van haar ex-werkgever om hem van overspel te beschuldigen. ('Rechter gaf voorbeeldstraf om sociale netwerksites te beschermen', *Knack* 21 september 2011. Te raadplegen op: http://datanews.knack.be/ict/nieuws/nieuwsoverzicht/2011/09/21/rechter-gaf-voorbeeldstraf-om-sociale-netwerksites-te-beschermen/article-1195107501639.htm)

[11] E. LIEVENS, *Protecting Children in the Digital Era. The Use of Alternative Regulatory Instruments,* Leiden en Boston, Martinus Nijhoff Publishers, 2010, International Studies in Human Rights, Vol. 105, 274, 315-316. (Hierna: E. LIEVENS, *Protecting Children*).

[12] Folder te raadplegen op: http://www.wdmcentral.be/wp-content/uploads/2011/03/White-Paper-Social-Media-Barometer1.pdf.

[13] VALGAEREN stelt sociale netwerkdiensten voor als digitale bijenkorven waarbij tal van diensten, producten en spelers betrokken zijn. (E. VALGAEREN, 'Sociale netwerksites – De digitale bijenkorven. Korte inleiding op het themanummer Sociale-netwerksites', *Computerr.* 2010/3, 94.)

maar weinig rechtspraak met betrekking tot SNS en privacy beschikbaar. Om enige wettelijke waarborgen ter bescherming van de privacy van minderjarigen te garanderen is men genoodzaakt terug te vallen op de bestaande privacyregelgeving. Nochtans blijkt uit een onderzoek van Unisys in 2011 dat drie kwart van de Belgen regulering van sociale media ter bescherming van hun online privacy een noodzaak vindt. Eén op de vier Belgen vindt dat het aan de overheid is om sociale media te reguleren terwijl één op de tien erop vertrouwt dat de sector zelf de nodige beschermingsmaatregelen neemt.[14]

Onderzoeksvragen en overzicht

5. In een eerste hoofdstuk wordt op een beknopte wijze de situatie van minderjarigen en SNS geschetst en wordt het bestaande wettelijke privacykader toegelicht. Het zwaartepunt ligt hier bij de Europese regelgeving.[15] Momenteel is op het niveau van de Europese Unie (EU) nog steeds de Richtlijn Bescherming Persoonsgegevens van 1995 van kracht. Omdat deze richtlijn niet meer in staat blijkt te zijn het hoofd te bieden aan de nieuwe sociale en economische realiteit van het internet, werd op 25 januari 2012 een voorstel voor een algemene gegevensbeschermingsverordening gedaan tot wijziging van de bestaande EU-regels.[16] De nieuwe bepalingen van de ontwerptekst die van belang zijn voor minderjarigen en SNS zullen in een tweede hoofdstuk worden geanalyseerd en geëvalueerd.

6. Het lijkt mij interessant een kijkje te nemen over de Atlantische Oceaan en het systeem van de Verenigde Staten onder de loep te nemen. In 1998 werd door het Amerikaanse Congres de Children's Online Privacy Protection Act (COPPA) aangenomen die een specifiek wettelijk kader in het leven riep ter bescherming van de persoonsgegevens op internet van kinderen onder de dertien jaar.[17] Toch kampt men tegenwoordig met dezelfde problemen als op het Europese continent. Een aantal jaren later bleek immers dat ook de COPPA niet meer het hoofd kon bieden aan de privacygerelateerde problemen van de nieuwe sociale media.

---

[14] De studie 'Unisys Security Index' is te raadplegen op: http://www.unisyssecurityindex.com/usi/belgium/news.

[15] Er dient opgemerkt te worden dat de Belgische Wet Bescherming Persoonsgegevens (zie randnummer 34) niet altijd toepasbaar is op SNS van buiten de EU aangezien die vaak de wet toepassen van het land waar ze hun maatschappelijke zetel hebben. Zo valt Netlog wel onder de Belgische wet, maar niet Facebook. De overeenkomst die men afsluit bij het aanmaken van een Facebookprofiel valt eigenlijk onder de Californische Wet. ('Beperk uw digitale voetafdruk', nieuwsbrief Test-Aankoop, maart 2010, te raadplegen op: http://mcs.test-aankoop.be/default.aspx?show=1351&src=645203&lge_id_c=N&prm_id_c=TANLSG&cop_id_c=N1004.01.)

[16] Voorstel voor een verordening van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (algemene verordening gegevensbescherming), 25 januari 2012, COM/2012/11 (Commissiedocument nr. 11 van 2010, definitieve versie). Te raadplegen op: http://ec.europa.eu/justice/data-protection/document/review2012/_com_2012_11_nl.pdf.

[17] http://www.ftc.gov/privacy/coppafaqs.shtm.

7. Uit beleidsdocumenten van de EU en de Raad van Europa blijkt dat men de online bescherming van minderjarigen de laatste jaren meer en meer wenst te verwezenlijken via sensibilisering, technische beveiligingsmaatregelen, zelfregulering en co-regulering.[18] In een derde hoofdstuk zullen twee recente alternatieve beleidsinitiatieven betreffende de veiligheid op SNS worden toegelicht. Zo werd in 2009 een zelfregulerende samenwerkingsovereenkomst gesloten tussen de Europese Commissie en de grootste sociale netwerken (de 'Safer Social Networking Principles for the EU').[19] Zeer recent werd een aanbeveling aangenomen door de Raad van Europa over de bescherming van mensenrechten met betrekking tot sociale netwerkdiensten.[20]

8. De centrale onderzoeksvraag van deze masterproef kan als volgt worden geformuleerd: zal het nieuwe voorstel voor een verordening betreffende de persoonsgegevensbescherming tot een meer effectieve bescherming van de privacy van minderjarigen op SNS kunnen leiden? Met name zal worden onderzocht wat de verbeteringen van het nieuwe voorstel zijn tegenover de huidige regels. Daarnaast zullen de tekortkomingen van de ontwerptekst worden nagegaan en wat de rol van alternatieve regulering hierbij kan zijn. Bovendien wordt onderzocht hoe de systemen van zelf- en co-regulering de leemtes in het wetgevende kader kunnen opvullen. Wat is uiteindelijk de beste wijze van regulering: overheidsregulering, alternatieve regulering of een combinatie van beide systemen? Kan men zich hiervoor inspireren op de Amerikaanse COPPA of op andere wetgeving ter bescherming van minderjarigen? Is het blijven uitwerken van alternatieve reguleringsinstrumenten aangewezen in dit domein of dient men uiteindelijk te streven naar een volledige integratie van de nieuwe vormen van sociale media en de privacygevoelige kwesties in het bestaande wettelijke kader van persoonsgegevensbescherming? *Fortasse erit, fortasse non erit…*

---

[18] Deze alternatieve reguleringsinstrumenten ('ARI's of 'Alternative Regulatory Instruments') werden uitgebreid geanalyseerd door Eva Lievens in haar doctoraat over de bescherming van minderjarigen tegen schadelijke media-inhoud. Zie: E. LIEVENS, *Protecting Children*, *supra* noot 11. Eva Lievens is wetenschappelijk medewerker verbonden aan het ICRI (Interdisciplinair Centrum voor Recht en ICT) van de KULeuven.

[19] 'Safer Social Networking Principles for the EU', 10 februari 2009. Te raadplegen op: http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf.

[20] Recommendation CM/Rec(2012)4 of the Committee of Ministers to member States on the protection of human rights with regard to social networking services, 4 april 2012. Te raadplegen op: https://wcd.coe.int/ViewDoc.jsp?id=1929453&Site=CM.

HOOFDSTUK 1. BEGRIPPEN, JURIDISCH KADER EN TOEPASSINGS-GEBIED

9. Vooraleer de voor minderjarigen en SNS relevante bepalingen van het voorstel tot verordening worden geanalyseerd en de aanvullende werking van alternatieve SNS-beleidsinstrumenten wordt onderzocht, zullen onder dit eerste hoofdstuk een aantal begrippen worden verduidelijkt. Ten eerste zal kort ingegaan worden op de positie van de minderjarige in de online bescherming en de (vooral Europese) beleidsinitiatieven die werden aangenomen hieromtrent (Afdeling 1). Vervolgens zal kort het fenomeen van SNS worden besproken vanuit juridisch perspectief (Afdeling 2) om dan ten slotte het bestaande privacykader te schetsen en toe te passen op de context van minderjarigen en SNS (Afdeling 3).

Afdeling 1. De online bescherming van minderjarigen

1. Minderjarigen

10. Er zijn niet zozeer opmerkelijke juridische implicaties of verschillen tussen de termen 'kind', 'adolescent', 'tiener' en 'jongere' wanneer men het heeft over minderjarigen. De meest gangbare termen zijn 'kind' of 'jongere' en hierbij is het beslissende criterium niets anders dan de leeftijd. In de meeste nationale wetgeving, verdragen en beleidsdocumenten is achttien jaar de leeftijd waarop men meerderjarig wordt.[21] Men spreekt meestal van 'kinderen' voor minderjarigen onder de dertien jaar (zoals in de Amerikaanse COPPA en in artikel 8 van het nieuwe voorstel tot verordening (zie randnummers 37 en 61)) en van 'jongeren' voor minderjarigen tussen dertien en zeventien jaar.[22]

In de sociale wetenschappen hanteert men leeftijdscategorieën naargelang de cognitieve ontwikkeling van het kind gaande van baby, peuter, kleuter, schoolkind naar puber. Ook in specifieke mediawetgeving en vormen van co- en zelfregulering zijn voorbeelden van dergelijke indeling te vinden. Zo onderscheidt het Nederlandse Kijkwijzersysteem vijf leeftijdsgroepen: alle leeftijden, afgeraden voor kinderen jonger dan zes jaar, afgeraden voor kinderen jongeren dan negen jaar, niet geschikt voor mensen jonger dan twaalf jaar en niet geschikt voor mensen jonger dan zestien jaar.[23] Verder in deze masterproef zullen de termen 'kind', 'jongere' en 'minderjarige' door elkaar gebruikt worden naargelang de context.

2. Het belang van het kind

11. Het 'belang van het kind' is niet alleen een belangrijke overweging uit de jeugdzorg of het familierecht, maar is ook een internationaal rechtsbegrip. Het principe is verankerd in artikel 3, 1ste lid van het VN-Kinderrechtenverdrag dat luidt: 'bij alle maatregelen betreffende kinderen, ongeacht of deze worden genomen door openbare of particuliere instellingen voor maatschappelijk welzijn of door rechterlijke instanties, bestuurlijke autoriteiten of wetgevende lichamen, vormen *de belangen van het kind* de eerste overweging'.

In het licht van de doelstellingen van de Europese Commissie in haar mededeling 'Naar een EU-strategie voor de rechten van het kind' onderzoekt de Werkgroep Gegevensbescherming Artikel 29 (verder: WG 29) in haar Advies 2/2009 naast

---

[21] E. LIEVENS, *Protecting Children*, *supra* noot 11, 27-28. Zo definieert artikel 1 van het VN-Kinderrechtenverdrag het kind als 'ieder mens jonger dan achttien jaar, tenzij volgens het op het kind van toepassing zijnde recht de meerderjarigheid eerder wordt bereikt'. Het Cybercrimeverdrag van de Raad van Europa definieert in zijn artikel 9.3 'minderjarigen' als alle personen onder de achttien jaar. Volgens artikel 388 van het Belgische Burgerlijk Wetboek is de minderjarige 'de persoon van het mannelijke of vrouwelijke geslacht die de volle leeftijd van achttien jaren nog niet bereikt heeft'.

[22] Een gelijkaardig onderscheid vind men terug in artikel 2, 15° en 18° van het Decreet betreffende radio-omroep en televisie van 27 maart 2009 (het Vlaamse Mediadecreet) waarin een 'jongere' gedefinieerd wordt als een persoon vanaf twaalf jaar tot onder de leeftijd van zestien jaar en een 'kind' als een persoon onder de leeftijd van twaalf jaar.

[23] Zie: http://www.kijkwijzer.nl/ index.php?id=93.

de kwestie van schoolgegevens de implicaties van de regelgeving betreffende de persoonsgegevensbescherming op de situatie van kinderen.[24] Zoals *infra* zal worden aangetoond ontbreken er momenteel specifieke bepalingen over het recht op privéleven van minderjarigen in het huidige Europese regelgevend kader. De Richtlijn Bescherming Persoonsgegevens (zie randnummers 25-31) is volgens de werkgroep niettemin van toepassing op elke 'natuurlijke persoon' en dus ook op minderjarigen. De bepalingen van deze richtlijn dienen dan ook op een strikte wijze toegepast te worden overeenkomstig het beginsel van het belang van het kind. Er moet hierbij rekening worden gehouden worden met de specifieke situatie van minderjarigen en van hun vertegenwoordigers.[25]

3. Beleidsinitiatieven ter bescherming van minderjarigen op internet

12. Om de lidstaten bewust te maken van de nieuwe uitdagingen rond de bescherming van minderjarigen in de online omgeving werd vanaf de jaren negentig door de Europese instanties heel wat aandacht besteed aan deze problematiek.[26] Een eerste EU-mededeling over de illegale en schadelijke inhoud op internet kwam er in 1996.[27] In 1998[28] en 2006[29] werden twee aanbevelingen

[24] Werkgroep Gegevensbescherming Artikel 29, Advies 2/2009 over de bescherming van persoonsgegevens van kinderen (Algemene richtlijnen en het bijzondere geval van scholen), 11 februari 2009, 5. Te raadplegen op: 9http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/ wp160_nl.pdf., 6. (Hierna: WG 29, Advies 2/2009)

[25] WG 29, Advies 2/2009, *supra* noot 24, 7 en 20.

[26] E. LIEVENS, 'Bescherming minderjarigen online', *supra* noot 5, 59.

[27] Mededeling van de Commissie aan de Raad, het Europees Parlement, het Economisch en Sociaal Comité en het Comité van de Regio's over de illegale en schadelijke inhoud op internet, COM(96)487.

[28] De aanbeveling van 1998 vloeide voort uit de consultatie over het Groenboek over de bescherming van minderjarigen en de menselijke waardigheid in de context van de audiovisuele en informatiediensten en was het eerste instrument betreffende de inhoud van audiovisuele en informatiediensten dat zich in zijn vijfde overweging specifiek richt op de bescherming van minderjarigen. De nadruk in deze aanbeveling ligt heel sterk op zelfregulering waarbij het opstellen van gedragscodes, het opzetten van technische systemen zoals filters en leeftijdsverificatiesystemen en samenwerking tussen de belanghebbenden wordt aangemoedigd. (Aanbeveling van de Raad van 24 september 1998 betreffende de ontwikkeling van de concurrentiepositie van de Europese industrie van audiovisuele en informatiediensten door de bevordering van nationale kaders teneinde een vergelijkbaar en doeltreffend niveau van bescherming van minderjarigen en de menselijke waardigheid te bereiken, *Pb.L.* 270, 7 oktober 1998, 48-55) Zie: E. LIEVENS, 'Bescherming minderjarigen online', *supra* noot 5, 60. In de aanloop naar de aanbeveling van 2006 verschuift de klemtoon iets meer naar co-regulering, zijnde een samenwerking tussen de overheid, de sector en andere belanghebbende partijen, dat volgens de Europese Commissie beter aangewezen is om de doelstellingen in verband met de bescherming van minderjarigen te verwezenlijken. (Tweede evaluatieverslag van de Commissie voor de Raad en het Europees Parlement van 12 december 2003 over de toepassing van de aanbeveling van de Raad van 24 september 1998 over de bescherming van minderjarigen en de menselijke waardigheid, COM(2003)/776, 3.)

[29] Aanbeveling van het Europees Parlement en de Raad van 20 december 2006 betreffende de bescherming van minderjarigen en de menselijke waardigheid en het recht op weerwoord in verband met de concurrentiepositie van de Europese industrie van audiovisuele en online-informatiediensten, *Pb.L.* 378, 27 december 2006, 72-77. In de aanbeveling van 2006 wordt overwogen dat zelfregulering *an sich* niet voldoende is om minderjarigen te beschermen tegen boodschappen met een schadelijke inhoud en dat de ontwikkeling van een Europese audiovisuele ruimte zou moeten stoelen op een permanente dialoog tussen nationale en Europese wetgevers, reguleringsinstanties, bedrijven, verenigingen, burgers en maatschappelijke organisaties. Als aanvulling op de aanbeveling van 1998 worden in deze aanbeveling de lidstaten opgeroepen om passende randvoorwaarden te creëren waarbij de focus zowel op co- als op zelfregulering ligt. Zie:

goedgekeurd. In een verslag van 2011 over de toepassing van de aanbevelingen van 1998 en 2006 verwijst de Europese Commissie naar de nieuwe ontwikkelingen, w.o. de opkomst van SNS, die zowel voor individuele gebruikers als in maatschappelijk opzicht enorm belangrijk zijn geworden.[30] Bij beschikking werd in 1999 door het Europees Parlement en de Raad het zgn. 'Actieplan Veiliger Internet' goedgekeurd voor een periode van vier jaar (van 1 januari 1999 tot 31 december 2002).[31] In 2005 werd dit plan opgevolgd door het programma 'Safer Internet Plus' ('voor een veiliger internet') met een looptijd van 2005 tot 2008 om in het licht van de nieuwe online technologieën een veiliger gebruik van het internet te bevorderen.[32] In december 2011 vormden 28 bedrijven een nieuwe coalitie om het internet 'een betere plek voor onze kinderen' te maken.[33] SNS zoals Facebook en Netlog hebben zich hierbij aangesloten.[34] De twee belangrijkste recente initiatieven die zich specifiek richten op SNS zijn de 'Safer Social Networking Principles for the EU' en de

---

Verslag van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's over de toepassing van de aanbeveling van de Raad van 24 september 1998 betreffende de bescherming van minderjarigen en de menselijke waardigheid en van de aanbeveling van het Europees Parlement en de Raad van 20 december 2006 betreffende de bescherming van minderjarigen en de menselijke waardigheid en het recht op weerwoord in verband met de concurrentiepositie van de Europese industrie van audiovisuele en online-informatiediensten – Bescherming van kinderen in de digitale wereld-, COM(2012)/0556 definitief, te raadplegen op: http://eur-lex.europa.eu/LexUriServ/ LexUriServ.do?uri=COM: 2011:0556: FIN:NL:HTML. (Hierna: Verslag Commissie, Bescherming kinderen digitale wereld)

[30] Verslag Commissie, Bescherming kinderen digitale wereld, *supra* noot 29.

[31] Beschikking 276/99/EG van het Europees Parlement en de Raad van 25 januari 1999 tot vaststelling van een communautair meerjarenactieplan ter bevordering van een veiliger gebruik van Internet door het bestrijden van illegale en schadelijke inhoud op mondiale netwerken. In 2003 werd het plan met twee jaar verlengd. Het programma had drie grote actielijnen: (1) het tot stand brengen van een veiliger klimaat door de oprichting van een Europees netwerk van directe klachtenlijnen (zgn. 'hotlines'), de bevordering van zelfregulering en de uitwerking van gedragscodes, (2) de ontwikkeling van filtersystemen en (3) bewustmakingsacties.

[32] Beschikking 2005/854/EG van het Europees Parlement en de Raad van 11 mei 2005 tot vaststelling van een communautair meerjarenprogramma ter bevordering van een veiliger gebruik van het internet en nieuwe online-technologieën. In tegenstelling tot het vroegere programma richtte het nieuwe plan zich veel meer tot de eindgebruikers zoals ouders, opvoeders en kinderen. (Zie: E. LIEVENS, *Protecting Children, supra* noot 11, 129) Het programma voorzag vier actielijnen: (1) het bestrijden van illegale inhoud waar bij de al eerder vermelde 'hotlines' aangifte kan worden gedaan van illegale inhoud, (2) de aanpak van ongewenste en schadelijke inhoud waarbij technologische maatregelen zoals filtering en inhoudsbeoordelingssystemen het hoofd moeten bieden aan de bestrijding van deze inhoud en waarbij het gebruik van privacyversterkende technologische maatregelen worden aangemoedigd, (3) het bevorderen van een veiligere omgeving met het opzetten van een effectief zelfreguleringssysteem en een 'Safer Internet Forum' en (4) bewustmakingsacties.

[33] Europese Commissie, Persbericht, 'Digitale Agenda: Coalitie van technologische topbedrijven en media om het internet een betere plek voor onze kinderen te maken, 1 december 2011. Te raadplegen op: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/1485&format=HTML&aged=0&language=EN&guiLanguage=en. In dit vrijwillig samenwerkingsinitiatief, eveneens een zelfregulerend instrument, werden de volgende beleidslijnen uitgestippeld: (1) eenvoudige en solide rapportage-instrumenten voor schadelijke inhoud, (2) aan de leeftijd aangepaste privacy-instellingen, (3) een ruimer gebruik voor inhoudsbeoordeling via leeftijdsclassificatie, (4) een uitbreiding van de beschikbaarheid en het gebruik van ouderlijk toezicht en (5) een efficiënte verwijdering van materiaal over kindermisbruik.

[34] E. LIEVENS, P. VALCKE en P.J. VALGAEREN, 'State of the art on regulatory trens in media. Identifying whether, what, ho wand who to regulate in social media', ICRI KULeuven, december 2011, 52. Te raadplegen op: http://emsoc.be/2552-conclusions-building-blocks-for-the-creation-of-regulatory-strategies-for-social-media/. (Hierna E. LIEVENS e.a., 'State of the art')

Aanbeveling van 4 april 2012 van de Raad van Europa (zie randnummers 96-104).

Afdeling 2. Sociale netwerksites

1. Web 2.0. en 'user-generated content'

13. SNS kaderen onder de nieuwe vormen van sociale media en vallen onder te brengen in de categorie van de zgn. 'Web 2.0.'-toepassingen.[35] Het internet is in een tijdspanne van tien jaar geëvolueerd van een eenvoudig informatieplatform naar een interactief communicatiemedium. Het sociale medialandschap wordt vandaag gestuurd door gebruikers en consumenten die niet enkel veel meer controle hebben gekregen over de inhoud die ze willen gebruiken, maar ook zelf de inhoud aanbieden en genereren: het zijn a.h.w. 'prosumers'.[36] Dit fenomeen van 'user-generated content' (afgekort: UGC en letterlijk vertaald: 'door gebruikers gegenereerde inhoud') heeft de culturele en economische organisatie en structuur van het internet aanzienlijk veranderd.[37]

De volgende stap in de evolutie van het internet zou 'Web 3.0.' of het zgn. 'semantische web' zijn waarbij door middel van technische integratie van netwerkdiensten en door open technologieën verschillende toepassingen aan elkaar gelinkt zouden kunnen worden.[38] Het huidige Web 2.0.-internetlandschap en de evolutie naar Web 3.0. is één van de belangrijkste redenen waarom het uitvaardigen van specifieke wetgeving betreffende de nieuwe vormen van sociale media geen gemakkelijke oefening is en in de toekomst alleen maar problematischer zal worden.

2. Definitie en kenmerken van SNS

14. In een advies van 2009 definieert de WG 29 een SNS als volgt: 'online communicatieplatformen waarop personen kunnen deelnemen aan netwerken

---

[35] Web 2.0. verwijst in de eerste plaats naar de tweede generatie online diensten waarbij gebruikers mede de inhoud bepalen die op het internet verschijnt. Web 2.0. is de opvolger van Web 1.0. waarbij het internet nog gekenmerkt werd door een eenrichtingsverkeer en voornamelijk gebruikt werd als een 'read only online folder' waarbij bedrijven en particulieren informatie op het web plaatsten dat via het internationale netwerk ('internet') beschikbaar werd gesteld. Web 2.0. is gericht op de interactie tussen gebruikers en hun dynamische deelname aan de inhoud op het internet. Web 2.0. hanteert de zgn. AJAX-ontwikkelingsmethode die verschillende technologieën omvat zoals HTML, CSS en XML. (zie: http://economie.fgov.be/nl/consument/Internet/telecommunicatie/web_2-0/) Internettechneut Tim O'Reilly bedacht de term in 2004 en situeert de omslag naar Web 2.0. in 2001 waarbij na het doorprikken van de 'internetbubble' de ganse ICT-sector een ferme deuk kreeg. (P. PETERSEN, *Handboek Online Marketing*, Amsterdam, Kluwer, 2009, 76 en 80.)

[36] E. LIEVENS e.a., 'State of the art', *supra* noot 34, 6.

[37] Deze nieuwe toepassing van het internet slaat vooral op het fenomeen van SNS maar ook op andere nieuwe vormen van sociale media zoals weblogs en sociale nieuwssites, 'crowdsourcing' en 'collective intelligence' zoals Wikipedia en 'sharing'-platformen zoals Youtube.

[38] P. PETERS, *Handboek Online Marketing*, Amsterdam, Kluwer, 2009, 76. Het internet is reeds aan het evolueren naar een Web 3.0.-systeem waarin data gedeeld en hergebruikt kan worden door verschillende applicaties, websites en gebruikersgroepen. Daardoor zou de uitwisseling van gegevens gemakkelijker verlopen en zou de data overal kunnen worden geraadpleegd. Een voorbeeld: op de gratis muziekstreamingssite Grooveshark van de Escape Media Group Inc. kan men zich aanmelden via Facebook, Twitter of Gmail (Google). (Zie ook: K. DEELSTRA, *Handboek Zoekmachinemarketing*, Zutphen, Koninklijke Whörmann, 2008, 384-385.)

van gelijkgezinde gebruikers of dergelijke netwerken kunnen opzetten'.[39] Een gelijklopende definitie is te vinden in de Amerikaanse literatuur: 'a website where registered users have the ability to log in and form connections both personally and professionally with other users'.[40] In de context van de 'Safer Social Networking Principles for the EU' (zie randnummers 95-100) worden de online diensten bedoeld die de volgende gemeenschappelijke kenmerken vertonen:

'(1) een platform dat sociale interactie via het internet stimuleert tussen twee of meerdere personen met de bedoeling om andere personen te ontmoeten, vrienden te maken of informatie uit te wisselen;

(2) een zekere mate aan functionaliteit die toelaat gebruikers een persoonlijke profielpagina op te stellen dat informatie omvat die ze zelf hebben gekozen, zoals de naam of 'nickname' van de gebruiker, afbeeldingen door de gebruiker geplaatst op de persoonlijke pagina van de gebruiker, andere persoonlijke informatie over de gebruiker en links naar andere persoonlijke pagina's op aanvraag van vrienden of collega's van de gebruiker die te raadplegen zijn door andere gebruikers of bezoekers;

(3) mechanismen om te communiceren met anderen, zoals een 'message board', elektronische e-mail of 'instant messenger' en

(4) 'tools' die de gebruiker in staat stellen andere gebruikers op te zoeken aan de hand van de profielinformatie die naar de keuze van deze laatste beschikbaar wordt gesteld voor andere gebruikers of bezoekers.'[41]

15. Door een enorme toename van SNS-gebruikers en de betrokkenheid van meer en meer economische spelers is de markt van de sociale netwerkdiensten geëvolueerd van een ontspannings- en reclamemedium naar een meer gespecialiseerd en doelgericht economisch instrument.[42] Dit fenomeen loopt parallel met de geleidelijke verschuiving van de inkomstenvergaring van sociale netwerken die hun inkomsten tegenwoordig niet alleen meer halen uit de

[39] Werkgroep Artikel 29, Advies 5/2009 over online sociaal netwerken, 12 juni 2009, 5. Te raadplegen op: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_nl.pdf. (Hierna: WG 29, Advies 5/2009)

[40] K. ANN BUB, 'Privacy's role in the discovery of social networking site information', *S.M.U.L. Rev.* 2011, 1435.

[41] 'Safer Social Networking Principles for the EU', 10 februari 2009. Te raadplegen op: http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf. In de eerste plaats is het samengesteld gebruikersprofiel de basistool waarin gebruikers hun persoonsgegevens centraliseren om een beschrijving van henzelf te voorzien met als doel contacten te verzamelen. Via uitnodigingen wordt het eigen profiel gekoppeld aan profielen van andere deelnemers om informatie te kunnen delen. Er wordt verder altijd een communicatiemogelijkheid voorzien via via mail, chatsessies, een elektronic bulletinboard etc. Ook wordt gretig gebruik gemaakt van advertenties die gerelateerd zijn aan het gegenereerde profiel ('targeted advertisements') waaruit sociale netwerkdiensten het grootste deel van hun inkomsten halen. R. VAN DEN HOVEN VAN GENDEREN, 'Sociale Netwerken, vloek of zegen? Algemene voorwaarden tot het gebruik van persoonlijke informatie', *Computerr.* 2010/3, 97. Het grootste gedeelte van de inkomsten uit reclame gaat zowel in de Verenigde Staten als op de internationale markt naar Facebook (http://www.digitale-media.be/index.php/headlines/advertenties-op-sociale-netwerken-brengen-binnen-2-jaar-10-miljard-dollar-op/) (Hierna: R. VAN DEN HOVEN VAN GENDEREN, 'Algemene voorwaarden')

[42] R. VAN DEN HOVEN VAN GENDEREN, 'Algemene voorwaarden', *supra* noot 41, 98.

commerciële advertenties maar steeds vaker een financiële vergoeding vragen aan de gebruikers.[43]

3. SNS vanuit juridisch perspectief

3.1 Algemene voorwaarden en privacy

16. In de meeste gevallen voorzien de aanbieders van sociale netwerkdiensten zichtbare privacy-opties waarbij de gebruiker de gewenste instellingen kan aanklikken. De algemene voorwaarden zijn echter meestal minder zichtbaar, maar zijn te raadplegen wanneer men een account aanmaakt op de gewenste SNS. Als men deze voorwaarden erop naleest, vindt men er bepalingen over o.a. instemming, dienstverlening, aansprakelijkheid, verantwoordelijkheid voor de inhoud van materiaal, de intellectuele eigendom van materialen en de beschikking over de informatie en de persoonlijke informatie die op SNS wordt getoond.[44] Het is dan ook voor de gebruikers van belang dat geldige en evenwichtige algemene voorwaarden worden opgesteld die in overeenstemming zijn met de wettelijke vereisten.[45] Via de algemene voorwaarden verleent de gebruiker de aanbieder immers een licentie om van de persoonlijke informatie gebruik te maken.[46]

3.2 Richtlijn Elektronische Handel en aansprakelijkheid

17. Belangrijk om te weten is in welke mate SNS-aanbieders aansprakelijk kunnen worden gesteld in geval van een miskenning van de algemene voorwaarden of overtreding van enige privacyregelgeving.[47] Aanbieders van sociale netwerkdiensten zouden in de eerste plaats kunnen aansluiten bij het begrip 'dienstverlener van de informatiemaatschappij' in de zin van de Richtlijn Elektronische Handel (ook wel de e-Commerce Richtlijn genoemd)[48]. Een dienst

---

[43] Vaak gebeurt dit geleidelijk. De deelnemer wordt na een bepaalde periode verwittigd van het feit dat hij, indien hij wil blijven gebruik maken van de sociale netwerkdiensten, een kleine vergoeding zal moeten betalen. Zie: A.R. LODDER, R. VAN DEN HOVEN VAN GENDEREN, A. ENGELFRIET, D. MEKIC e.a., 'Recht en Web 2.0', *Publicatiereeks NVvIR* No. 27, 2010, 21. Te raadplegen op: http://da.nny.nl/wp-content/uploads/2008/05/rechtenweb20.pdf. (Hierna: A.R. LODDER, 'Recht en Web 2.0.')

[44] A.R. LODDER e.a., 'Recht en Web 2.0.', *supra* noot 43, 86 en R. VAN DEN HOVEN VAN GENDEREN, 'Algemene voorwaarden', *supra* noot 41, 99. Helemaal onderaan rechts op bijvoorbeeld de webpagina van Facebook kunt U klikken op 'Privacy' en 'Gebruiksvoorwaarden'.

[45] R. VAN DEN HOVEN VAN GENDEREN, 'Algemene voorwaarden', *supra* noot 41, 99.

[46] R. VAN DEN HOVEN VAN GENDEREN, 'Algemene voorwaarden', *supra* noot 41, 97.

[47] Zo werd Facebook in 2008 aangeklaagd voor het schenden van de privacy van de gebruikers samen met het overtreden van computerfraudewetgeving. Facebook had een systeem ingesteld, het zgn. 'Beacon'-programma, waarbij de activiteiten van gebruikers werden bijgehouden en zichtbaar gemaakt voor andere bezoekers. In 2009 wijzigde Facebook de instellingen waardoor merkwaardig genoeg gegevens die gebruikers als privé hadden ingesteld nu openbaar werden voor alle Facebook-gebruikers. Alweer volgde een golf van aanklachten zodat Facebook uiteindelijk in 2010 de instellingen aanpaste teneinde gebruikers de mogelijkheid te geven om te bepalen voor wie welke gegevens toegankelijk zijn. Zie: A.R. LODDER e.a.,' Recht en Web 2.0.' , *supra* noot 43, 29.

[48] Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt ('richtlijn inzake elektronische handel'), *Pb.L.* 178, 17 juli 2000, 1-16. Op te merken valt dat sociale netwerkdiensten daarentegen niet vallen onder het toepassingsgebied van de Richtlijn Audiovisuele Mediadiensten (richtlijn 2010/13/EU van het

van de informatiemaatschappij wordt gedefinieerd als 'elke dienst die gewoonlijk tegen vergoeding, langs elektronische weg op afstand en op individueel verzoek van een afnemer van de dienst verricht wordt'.[49] Aanbieders van sociale netwerkdiensten zullen dientengevolge als tussenpersonen moeten voldoen aan de verplichtingen uit de richtlijn.

In beginsel kunnen aanbieders van sociale netwerkdiensten aansprakelijk worden gesteld indien de door hen opgeslagen informatie van hun gebruikers inbreuk maakt op rechten van anderen w.o. deze vervat in de privacyregelgeving.[50] In artikel 14 van de richtlijn is een aansprakelijkheidsvrijstelling voorzien voor de zgn. 'hosting providers'. Een SNS-aanbieder zou derhalve als 'hosting provider' niet aansprakelijk zijn voor de op verzoek van de afnemer van de dienst opgeslagen informatie indien hij 'niet daadwerkelijk kennis heeft van de onwettige activiteit of informatie en, wanneer het een schadevergoedingsvordering betreft, geen kennis heeft van feiten of omstandigheden waaruit het onwettig karakter van de activiteiten of informatie duidelijk blijkt (puntje a), of […]zodra hij van het bovenbedoelde daadwerkelijk kennis heeft of besef krijgt, prompt handelt om de informatie te verwijderen of de toegang daartoe onmogelijk te maken' (puntje b: de zgn. 'notice and take down'-verplichting).[51] Indien de dienstverlener niet onder deze aansprakelijkheidsbeperking valt, dient men terug te vallen op het gemeen aansprakelijkheidsrecht.

Op Europees niveau heerst er nogal wat onduidelijkheid over de kwalificatie van een sociale netwerkdienst als 'hosting provider' in de zin van artikel 14 van de Richtlijn Elektronische Handel. Ofschoon er afwijkende rechtspraak bestaat, kan een SNS-aanbieder m.i. onder deze 'safe harbour'-bepaling vallen. Het recent arrest van 16 februari 2012 (Sabam/Netlog) waarin het Hof van Justitie de Richtlijn Elektronische Handel (nl. het verbod van een algemene toezichtverplichting van artikel 15) als één van de rechtsgronden hanteerde waarop het zijn beslissing steunde, kan hier enigszins een argument voor zijn. (zie voetnoot 53). Bovendien stelde het Hof in zijn Google Adwords-rechtspraak dat de dienstverlener zich dient te beperken tot een neutrale levering van de dienst met behulp van een louter technische en automatische verwerking van de gegevens die hem door zijn klanten zijn verstrekt om zich te kunnen beroepen op de 'safe harbour'-bepaling.[52] Het is aannemelijk te stellen dat een sociale netwerkdienst een dergelijke passieve rol vervult. Wanneer potentieel

---

Europees Parlement en de Raad van 10 maart 2010 betreffende de coördinatie van bepaalde wettelijke en bestuursrechtelijke bepalingen in de lidstaten inzake het aanbieden van audiovisuele mediadiensten, *Pb.L* 95, 15 april 2010, 1-24) vallen aangezien de SNS-aanbieder geen redactionele verantwoordelijkheid uitoefent en een sociale netwerkdienst niet als hoofddoel het verspreiden van programma's heeft in de zin van artikel 1, a) van deze richtlijn.

[49] Artikel 2, a) van de richtlijn verwijst naar de definitie die omschreven is in artikel 1, lid 2, van Richtlijn 98/34/EG.

[50] A.R. LODDER e.a., 'Recht en Web 2.0.', *supra* noot 43, 85.

[51] Artikel 14, a) en b) van de Richtlijn Elektronische Handel.

[52] HvJ, 23 maart 2010, *Google/Vuitton e.a.*, C-236 tot C-238, punten 113, 114 en 120. Te raadplegen op: http://www.iept.nl/files/ 2010/IEPT20100323_HvJEU_Google_Adwords.pdf. Zie ook rechtsoverweging 42 van de Richtlijn Elektronische Handel.

onrechtmatige informatie op een SNS wordt geplaatst, zal de host van deze site bijgevolg niet aansprakelijk zijn zolang hij niet op de hoogte is of niet op de hoogte behoorde te zijn van de onrechtmatigheid van de informatie. In de praktijk zijn aanbieders van sociale netwerkdiensten echter snel geneigd om na een verzoek tot het verwijderen van bepaalde informatie de informatie van de site weg te halen om enige aansprakelijkheid te vermijden.[53]

Artikel 15 van de richtlijn stelt dat de lidstaten de dienstverlener van de informatiemaatschappij geen algemene verplichting mogen opleggen om toe te zien op de informatie die zij doorgeven of opslaan, noch om actief te zoeken naar feiten of omstandigheden die op onwettige activiteiten duiden. Aanbieders van SNS hoeven in principe dus niet te controleren wat wordt geplaatst op hun sites. Bovendien kunnen aanbieders hun aansprakelijkheid (deels) uitsluiten in de algemene voorwaarden.[54]

3.3 Elektronische communicatiediensten

18. Diensten van de informatiemaatschappij moeten onderscheiden worden van de 'elektronische communicatiediensten' in de zin van richtlijnen betreffende elektronische communicatie[55] en de wet van 13 juni 2005 betreffende de elektronische communicatie.[56]

In principe vallen sociale netwerkdiensten *an sich* buiten de definitie van 'elektronische communicatiedienst'.[57] Aanvullende diensten zoals het uitbaten van een chatbox of een instant messaging netwerk kunnen naast de kwalificatie van dienst van de informatiemaatschappij eveneens onder de definitie van een elektronische communicatiedienst vallen, omdat de infrastructuur waarvan zij gebruik maken en die uitgebaat wordt door een internettoegangsleverancier een dergelijke dienst uitmaakt.[58] Beide hoedanigheden kunnen dus in bepaalde gevallen samenlopen.

---

[53] A.R. LODDER e.a., 'Recht en Web 2.0.', *supra* noot 43, 85.

[54] In die lijn stelde het Europese Hof van Justitie in het reeds vermelde Sabam/Netlog-arrest van 16 februari 2012 dat een hostingdienstverlener (*in casu* de Belgische SNS Netlog) niet kan verplicht worden een algemeen filtersysteem te installeren tegen illegaal downloaden. In dit arrest moest de bescherming van het auteursrecht wijken voor o.a. de vrijheid van informatie en de bescherming van de persoonsgegevens. Zie: HvJ, 16 februari 2012, *SABAM/Netlog*, C-360/10. Te raadplegen op: http://www.iept.nl/files/ 2012/IEPT20120216HvJEU SABAM v Netlog.pdf.

[55] Zie voetnoot 81.

[56] *BS*, 20 juni 2005. In artikel 2, 5° van de omzettingswet wordt een elektronische communicatiedienst omschreven als 'een gewoonlijk tegen vergoeding aangeboden dienst die geheel of hoofdzakelijk bestaat in het overbrengen, waaronder schakel- en routeringsverrichtingen, van signalen via elektronische communicatienetwerken, '[…], met uitzondering van (b) de diensten van de informatiemaatschappij' zoals omschreven in artikel 2 van de wet van 11 maart 2003 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, die niet geheel of hoofdzakelijk bestaan uit het overbrengen van signalen via elektronische communicatienetwerken […]'. Elektronische communicatiediensten betreffen dus de fysieke infrastructuur waarlangs communicatie tot stand komt waar diensten van de informatiemaatschappij eveneens betrekking kunnen hebben op communicatie, maar altijd geleverd worden bovenop de elektronische communicatiediensten. (P. VAN EECKE (ed.), *Recht en elektronische handel*, Brussel, Larcier, 2011, 7.)

[57] WG 29, Advies 5/2009, *supra* noot 39.

[58] P. VAN EECKE (ed.), *Recht en elektronische handel*, Brussel, Larcier, 2011, 7.

Afdeling 3. Privacy, internet en kinderen: huidig wettelijk kader

1. Het recht op privacy

1.1 Artikel 8 EVRM

19. In het algemeen wordt aanvaard dat fundamentele mensenrechten evenzeer van toepassing zijn op kinderen en jongeren.[59] Artikel 8 van het Europees Verdrag voor de Rechten van de Mens (verder: EVRM) is één van de Europese kernbepalingen wat betreft het recht op privacy en is ook van toepassing op minderjarigen.[60]

Het artikel luidt als volgt:

'1. Een ieder 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 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, de bescherming van de gezondheid of de goede zeden, of voor de bescherming van de rechten en vrijheden van anderen.'

Naast de eerbiediging van het gezinsleven, het huis en de communicatie wordt het recht op de eerbiediging van het privéleven het vaakst ingeroepen en functioneert a.h.w. als een generieke term die de drie andere elementen omvat.[61] Het recht op privacy uit het EVRM heeft net zoals de andere bepalingen uit het verdrag directe werking in de Belgische rechtsorde, maar is een relatief recht. Dit betekent dat dit recht onderworpen kan worden aan beperkingen of inmengingen en in een bepaalde situatie niet zal worden toegepast wanneer het recht op privacy moet onderdoen voor de bescherming van een ander belang of recht zoals het recht op vrije meningsuiting. Artikel 8, lid 2 EVRM bevat een aantal specifieke gronden die de zgn. beperkingsclausule of escapeclausule vormen.[62] Dit betekent dat in geval van een beperking of inmenging de drie voorwaarden uit het tweede lid vervuld moeten zijn. De beperking zal gerechtvaardigd zijn wanneer het voorzien is bij wet (legaliteitstoets), hierbij een legitieme doelstelling wordt nagestreefd (legitimiteitstoets) en de beperking of inmenging noodzakelijk is in een democratische rechtsstaat (noodzakelijkheidstoets).[63]

---

[59] E. LIEVENS, *Protecting Children*, *supra* noot 11, 265.
[60] E. LIEVENS, *Protecting Children*, supra noot 11, 316.
[61] J. VANDE LANOTTE en Y. HAECK (eds.), *Handboek EVRM. Deel 2. Artikelsgewijze commentaar (Volume I)*, 2004, Antwerpen, Intersentia, 711. (Hierna: J. VANDE LANOTTE, *Handboek EVRM*)
[62] J. VANDE LANOTTE, *Handboek EVRM (Deel 1. Algemene beginselen)*, *supra* noot 59, 123.
[63] Dit toetsingsschema geldt niet enkel voor artikel 8 EVRM maar ook artikelen 9 t.e.m. 11 van het EVRM en artikel 2 Vierde Protocol bij het EVRM bevatten een dergelijke beperkingsclausule.

1.2 De zaak K.U. t. Finland

20. Ofschoon de beperkingsclausule van artikel 8 EVRM negatief is geformuleerd, wordt in de rechtspraak van het Europees Hof voor de Rechten van de Mens (verder: EHRM) vaak gewezen op de positieve verplichting van de verdragsstaten om de nodige maatregelen te nemen teneinde het genot van het privéleven te verzekeren.[64] Specifiek wat de bescherming van de persoonlijke levenssfeer van minderjarigen op het internet en de positieve verplichting van de staat betreft, deed het Europees Hof op 2 december 2008 uitspraak in een zaak tegen Finland en concludeerde dat artikel 8 EVRM was geschonden.[65]

De feiten waren de volgende. Een onbekende persoon had een advertentie van seksuele aard op het internet geplaatst waarbij de leeftijd en het geboortejaar van K.U., een twaalfjarige jongen, werden vermeld, vergezeld van een beschrijving van zijn uiterlijke kenmerken en een boodschap dat de minderjarige op zoek was naar een intieme relatie. Via een link kon men een foto van de minderjarigen en zijn telefoonnummer raadplegen. De jongen kwam dit weten nadat hij een e-mail had ontvangen van een geïnteresseerde man. Zijn vader verzocht de politie de identiteit te achterhalen van de persoon die de advertentie had geplaatst teneinde strafrechtelijke vervolging mogelijk te maken. De politie verzocht op zijn beurt de betrokken ISP om de identiteit kenbaar te maken, maar in eerste aanleg werd dit door een Finse rechtbank afgewezen. Zowel in hoger beroep als in cassatie werd deze beslissing bevestigd. K.U. trok dan maar naar het EHRM.[66]

De Finse autoriteiten stelden dat het op het ogenblik van de feiten op grond van de Finse wetgeving niet mogelijk was om de identiteit van de persoon te achterhalen. Het Hof wees op het feit dat het reeds algemeen bekend was dat het internet kon worden gebruikt voor dergelijke pedofiele doeleinden. Finland had moeten wetgeving uitvaardigen om kinderen te beschermen tegen pedofielen op het internet. Zij hadden de middelen moeten voorzien voor strafonderzoek en correctionele vervolging. Bovendien moet hierbij een afwe-

---

[64] O.a. in de volgende zaken: EHRM, Graham Gaskin v. United Kingdom, 7 juli 1989, *Publ.Hof*, Serie A, Vol. 160; EHRM, Mark Rees v. United Kingdom, 17 oktober 1986, *Publ.Hof*, Serie A, Vol.106 en EHRM, X. and Y. v. the Netherlands, 26 maart 1985, no. 8978/80. Te raadplegen op: http://www.coe.int/t/dg2/equality/domesticviolencecampaign/resources/x%20and%20y%20v%20the%20netherlands_EN.asp. In het arrest X en Y t. Nederland veroordeelde het Hof Nederland omdat in de interne wetgeving de mogelijkheid ontbrak om strafvervolging in te stellen tegen iemand die seksueel geweld pleegde op een mentaal gehandicapt meisje van 16 jaar. Lidstaten zijn op grond van artikel 8 EVRM verplicht maatregelen te nemen ter bescherming van de seksuele integriteit om het respect op het privéleven te verzekeren. (P. DE HERT, 'Systeemverantwoordelijkheid voor de informatiemaatschappij als positieve mensenrechtenverplichting', 41. Te raadplegen op: http://www.vub.ac.be/LSTS/pub/Dehert/Dehert_371_restricted.pdf.

[65] EHRM, K.U. v. Finland, 2 december 2008, no. 2872/02. Te raadplegen op: http://www.coe.int/t/dghl/standardsetting/dataprotection/Judgments/KU%20v%20Finland%20en%20presse.pdf.

[66] E. LIEVENS, *Protecting Children, supra* noot 11, 404 en D. VOORHOOF, 'Recente arresten van het EHRM in verband met artikel 10 EVRM (vrijheid van meningsuiting en informatie). Te raadplegen op: http://www.psw.ugent.be/Cms_global/uploads/publicaties/dv/06recente_publicaties_case_law/ AM.2009.01.EHRM.NovDec2008.20.04.pdf.

ging worden gemaakt tussen enerzijds het recht op privacy en het recht op vrijheid van meningsuiting van internetgebruikers en anderzijds het voorkomen van misdrijven en het beschermen van het recht op privacy van kinderen, aldus het Hof.[67] Het Hof oordeelde dan ook dat Finland gefaald had in zijn positieve verplichting op grond van artikel 8 EVRM om het recht op privacy van de betrokken minderjarige op het internet te beschermen.

21. Het arrest maakt vooreerst duidelijk dat het recht op anonimiteit[68] op het internet geen dekmantel mag zijn om de aansprakelijkheid voor misdrijven te ontlopen. Er zijn immers in de loop van de laatste tien jaar garanties ingebouwd in Europese en nationale wetgeving om in het kader van een strafrechtelijk onderzoek de identiteit of het IP-adres van de auteur van strafbare inhoud te achterhalen via de Internet Service Provider (ISP).[69]

22. Belangrijker voor deze masterproef is dat deze zaak aantoont dat door de bijkomende kwetsbaarheid van minderjarigen bij dergelijke cybergevaren een doorgedreven privacybescherming op internet onmisbaar is geworden.[70] Het belang van privacybescherming voor minderjarigen werd bovendien twee jaar later bevestigd in een arrest van 16 december 2010.[71]

Artikel 8 EVRM blijft dus een solide rechtsbasis voor de bescherming van de privacy van minderjarigen op het internet. Door zijn algemene bewoordingen is de bepaling beter bestand tegen de nieuwe online ontwikkelingen dan de principes in de Richtlijn Bescherming Persoonsgegevens (zie randnummers 25-31). Het nadeel hierbij is dat het EVRM moet worden geïnterpreteerd naargelang de omstandigheden. Bovendien kunnen de bepalingen enkel worden ingeroepen tegenover overheden (verticale werking) en kan het na de uitputting van de interne rechtsmiddelen jaren duren vooraleer men uiteindelijk de zaak voor het Europees Hof kan brengen.[72]

---

[67] Finland heeft sedert 2004 zijn wetgeving aangepast zodat voortaan de identiteit van de afzender kan worden achterhaald op het internet.

[68] Op het internet wordt nu eenmaal verkeerde, onbetrouwbare of lasterlijke informatie geplaatst. In principe kan degene die dergelijke informatie online beschikbaar stelt zich beroepen op het recht op anonimiteit dat erkend is in de Verklaring betreffende de expressievrijheid op het internet van de Raad van Europa van 2003 (Principe 7). (Te raadplegen op: http://www.coe.int/t/dghl/standardsetting/media/doc/CM/Dec(2003)FreedomCommInt_en.asp#TopOfPage.)

[69] D. VOORHOOF, 'Recente arresten van het EHRM in verband met artikel 10 EVRM (vrijheid van meningsuiting en informatie)', november-december 2008. Te raadplegen op: http://www.psw.ugent.be/Cms_global/uploads/publicaties/dv/06recente_publicaties_case_law/AM.2009.01.EHRM.NovDec2008.20.04.pdf.

[70] Zie o.a. § 41 van het arrest waarin het Hof stelt dat 'although this case is seen in domestic law terms as one of malicious misrepresentation, the Court would prefer to highlight these particular aspects of the notion of private life, having regard to the potential threat to the applicant's physical and mental welfare brought about by the impugned situation and to his vulnerability in view of his young age'.

[71] EHRM, 16 december 2010, Aleksey Ovchinnikov v. Rusland, no. 24061/04. Te raadplegen op: http://cmiskp.echr.coe.int/tkp197/viewhbkm.asp?sessionId=72196096&skin=hudoc-en&action=html&table=F69A27FD8FB86142BF01C1166DEA398649&key=40590&highlight=.

[72] A.R. LODDER, 'Recht en Web 2.0.', *supra* noot 43, 121.

1.3 Artikel 16 VN-Kinderrechtenverdrag

23. Op 20 november 1989 werd het Verdrag inzake de rechten van het kind aangenomen door de Algemene Vergadering van de Verenigde Naties (verder: VN-Kinderrechtenverdrag). Dit internationaal instrument voorziet een juridisch kader ter bescherming van de rechten van het kind. Artikel 16 van het Verdrag handelt over het recht op de eerbieding van het privéleven en luidt als volgt:

'1. Geen enkel kind mag worden onderworpen aan willekeurige of onrechtmatige inmenging in zijn privéleven, in zijn gezinsleven, zijn huis of zijn briefwisseling, noch aan enige onrechtmatige aantasting van zijn eer en goede naam.

2. Het kind heeft recht op bescherming door de wet tegen zodanige inmenging of aantasting.'

Ieder kind kan zich beroepen op deze bepaling en overheden zijn verplicht zich te onthouden van enige onrechtmatige inmenging in de persoonlijke levenssfeer van het kind. Deze bepaling moet door iedereen worden gerespecteerd, ook door de wettelijke vertegenwoordigers van het kind en de persoonlijke levenssfeer van het kind moet in elke situatie worden beschermd.[73] Het is van belang op te merken dat dit artikel evenzeer van toepassing is in de online informatie- en communicatieomgeving.[74]

24. Het VN-Kinderrechtenverdrag bevat geen efficiënt afdwingingsmechanisme, maar voorziet in een rapportageprocedure waarbij het VN-Comité voor de Rechten van het Kind op grond van artikel 43 van het Verdrag toeziet op de naleving van de verdragsbepalingen op basis van periodieke rapporten. Dit betekent dat kinderen niet rechtstreeks naar de rechter kunnen, maar dat het Verdrag wel een groot moreel gezag uitstraalt en hoofdzakelijk een symbolische functie heeft.[75]

2. Richtlijn Bescherming Persoonsgegevens

25. Persoonsgegevensbescherming is een belangrijk aspect van het recht op privacy, met name bij de praktijk van het bijhouden van persoonsgegevens in al dan niet private registers of databanken. Opgeslagen gegevens in databanken zijn immers vatbaar voor misbruik waardoor zich een miskenning van het recht op privacy kan voordoen.[76] Het individuele recht op bescherming van persoonsgegevens ligt sinds 2000 vervat in artikel 8 van het Handvest van de grondrechten van de Europese Unie.[77]

---

[73] WG 29, Advies 2/2009, *supra* noot 24, 5.
[74] E. LIEVENS, *Protecting Children*, *supra* noot 11, 315-316.
[75] E. LIEVENS, *Protecting Children*, *supra* noot 11, 279.
[76] J. VANDE LANOTTE, *Handboek EVRM (Deel 2)*, *supra* noot 59, 735. Onder auspiciën van de Raad van Europa werd in 1981 een aanvullend verdrag gesloten: het zgn. Dataprotectieverdrag. Dit verdrag is een uitwerking van het recht op eerbiediging van het privéleven van artikel 8 EVRM voor de bescherming van persoonsgegevens bij geautomatiseerde verwerking en is de aanzet geweest tot het uitvaardigen van de Belgische Wet Bescherming Persoonsgegevens van 1992 (zie randnummer 34).
[77] Het Handvest is te raadplegen op: http://www.europarl.europa. eu/charter/pdf/text_nl.pdf.

Persoonsgegevens worden tegenwoordig op allerhande manieren verzameld. Hieronder wordt het bestaande EU-instrument betreffende gegevensbescherming kort toegelicht. In Hoofdstuk 2 wordt vervolgens het nieuwe voorstel van begin dit jaar tot wijziging van de bestaande regels uitgebreid besproken in het licht van de bescherming van minderjarigen op SNS.

2.1 Achtergrond

26. Op het niveau van de EU werd op 24 oktober 1995 de Richtlijn betreffende de bescherming van persoonsgegevens (ook wel de Privacyrichtlijn genoemd en verder afgekort als RBP) aangenomen.[78] De richtlijn kwam er in een tijdperk waarin men steeds vaker gebruik ging maken van verwerking van persoonsgegevens (overweging 4) en meer en meer gegevens werden uitgewisseld tussen ondernemingen die in verschillende lidstaten zijn gevestigd (overweging 5). Men was zich tevens bewust van de technologische ontwikkelingen in de informatiemaatschappij en de verschuiving naar de elektronische communicatie (overweging 6).

De richtlijn voorziet een algemeen kader voor de verwerking van persoonsgegevens en tracht een hoog niveau van persoonsgegevensbescherming en het vrij verkeer van persoonsgegevens in de Europese Unie te bewerkstelligen (artikel 1 RBP). Men heeft tegelijkertijd getracht strenge beperkingen te stellen aan het verzamelen en verwerken van persoonsgegevens.

2.2 Toepassingsgebied

27. De richtlijn is van toepassing op de verwerking van persoonsgegevens, ongeacht of deze verwerking geautomatiseerd is of niet (artikel 3). De bescherming van persoonsgegevens dient technologieneutraal te zijn om ontduiking te voorkomen. De verzameling en verwerking van persoonsgegevens op sociale netwerkdiensten valt in beginsel onder het toepassingsgebied.

28. In artikel 2 zijn een aantal definities opgenomen. Persoonsgegevens worden omschreven als 'iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon […] die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatienummer of van een of meer specifieke elementen die kenmerkend zijn voor zijn of haar fysieke, fysiologische, psychische, economische, culturele of sociale identiteit'.[79] Verder worden ook 'verwerking van persoonsgegevens' en 'toestemming van de betrokkene' gedefinieerd.

[78] Richtlijn 95/46/EG betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, *Pb.L.*, 23 november 1995, afl. 281, 31-50. De richtlijn werd aangevuld door Kaderbesluit 2008/977/JBZ van de Raad van 27 november 2008 over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politiële en justitiële samenwerking in strafzaken, *Pb.L.* 350, 30 december 2008, 60 e.v. (Hierna: RBP)

[79] Artikel 2, a) RBP.

2.3 Beginselen inzake de rechtmatigheid van de verwerking

29. De richtlijn bevat een aantal principes op basis waarvan de rechtmatigheid van de verwerking van persoonsgegevens wordt bepaald. Deze beginselen hebben vooreerst betrekking op de kwaliteit van de gegevens. Op grond van artikel 6 RBP moeten de lidstaten bepalen dat de persoonsgegevens eerlijk en rechtmatig, voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden moeten worden verwerkt en niet worden verwerkt op een wijze die onverenigbaar is met die doeleinden (het zgn. finaliteitsbeginsel). De gegevens moeten bovendien nauwkeurig zijn en, indien nodig, dienen ze te worden bijgewerkt. Artikel 7 slaat op de toelaatbaarheid van de verwerking en is de uitwerking van het proportionaliteitsbeginsel. Er mogen niet meer gegevens worden verwerkt dan noodzakelijk om het doel te bereiken. Artikel 8 regelt een aantal bijzondere categorieën van gegevens. Zo moet de verwerking van persoonsgegevens waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging, of het lidmaatschap van een vakvereniging blijkt, alsook de verwerking van gegevens die de gezondheid of het seksuele leven betreffen, worden verboden.

Op grond van de artikelen 10 en 11 moet elke betrokkene redelijkerwijze worden geïnformeerd over de gegevens die worden verwerkt (hieruit kan het transparantiebeginsel worden afgeleid). Krachtens artikel 12 heeft de betrokkene een recht van toegang tot de gegevens en een recht van rectificatie en uitwissing of afscherming van de gegevens. Artikel 13 bepaalt de uitzonderingen en beperkingen op de beginselen betreffende de kwaliteit van de gegevens, de informatieverstrekking aan de betrokkene, het recht van toegang en de openbaarheid van de verwerking. Artikel 14 voorziet een recht van verzet voor de betrokkene. Artikel 16 legt het vertrouwelijkheidsbeginsel vast en artikel 17 het principe van de beveiliging van de verwerking. Artikel 18 voorziet voor de verantwoordelijke voor de verwerking een meldingsplicht bij de nationale toezichthoudende autoriteit die opgericht moest worden op grond van artikel 28 (in België: de Commissie voor de Bescherming van de Persoonlijke Levenssfeer (verder: CBPL). De RBP bevat ten slotte nog een aantal formele en procedurele bepalingen.

30. De RBP is nog steeds de hoeksteen van gegevensbescherming in de Europese Unie en is uiteraard van toepassing op online gegevensverwerking. Het Nederlandse College Bescherming Persoonsgegevens stelde in haar richtsnoeren van 2007[80] dat 'persoonsgegevens op internet op dezelfde zorgvuldige wijze moeten worden verwerkt als in de offlinewereld'. Men dient als verantwoordelijke van gegevensverwerking en als betrokkene in een online omgeving evenzeer behoorlijk en zorgvuldig te werk te gaan en de beginselen van transparantie, finaliteit, kwaliteit en proportionaliteit te respecteren. *Infra* worden de relevante bepalingen van de RBP toegepast op de context van minderjarigen en SNS (zie randnummers 46-56).

[80] Te raadplegen op: http://www.cbpweb.nl/downloads_rs/rs_20071211_persoonsgegevens_op_internet_definitief.pdf.

2.4 Geen specifieke bepalingen betreffende minderjarigen

31. Het is logisch dat men anno 1995 nog niet dacht aan het fenomeen van SNS. De invloed van het internet op de samenleving was toen immers veel beperkter dan nu.

Het ontbreken van enige bijzondere bepalingen inzake de bescherming van persoonsgegevens van minderjarigen of kinderen is niettemin betreurenswaardig. De bepalingen van de huidige richtlijn zijn uiteraard wel van toepassing op minderjarigen, maar een aantal kind-specifieke beschermingsbepalingen ware wenselijk geweest. De ontwerptekst van de toekomstige verordening voorziet nu wel een aantal specifieke bepalingen die de kwetsbare positie van minderjarigen op het internet in rekening nemen (zie randnummers 59-72).

3. De e-Privacy richtlijn[81]

32. De richtlijn Privacy en Elektronische Communicatie van 12 juli 2002 (ook wel de e-Privacy Richtlijn genoemd) is volgens zijn artikel 1 een aanvulling en concretisering op de RBP voor de sector elektronische communicatie en wil eveneens een gelijk niveau van bescherming van het recht op privacy garanderen in de lidstaten.[82] Voor de sector van SNS is deze richtlijn slechts in beperkte mate relevant aangezien sociale netwerkdiensten als zodanig niet onder de definitie van een 'elektronische communicatiedienst' vallen (zie randnummer 18).

4. Privacybescherming in het Belgisch recht

4.1 Artikel 22 van de Grondwet

33. Het recht op privacy werd in 1994 ingeschreven in de Belgische Grondwet. Het eerste lid van artikel 22 GW bepaalt dat iedereen het recht heeft op

[81] Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector van elektronische communicatie, *Pb.L.* , 31 juli 2002, afl. 201, 37-47. Deze richtlijn vormt een onderdeel van de zgn. 'elektronische communicatierichtlijnen' uit 2002 waarbij de EU de voorwaarden heeft willen harmoniseren waaronder men in de Europese interne markt netwerken kan aanleggen en netwerkdiensten kan aanbieden. Deze richtlijn wilde het hoofd bieden aan de opmars van nieuwe digitale uitdagingen en legt de focus op veiligheid van de diensten en vertrouwelijkheid van de informatie. In 2009 werd de richtlijn gewijzigd (richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009 tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronischecommunicatienetwerken en -diensten, Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie en Verordening (EG) nr. 2006/2004 betreffende samenwerking tussen de nationale instanties die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming, *Pb.L.* 337, 18 december 2009, 11-36) waarbij een 'opt-in'-regel voor cookies werd geïntroduceerd, een meldplicht voor datalekken, de mogelijkheid voor providers om in rechte op te treden tegen spammers en een bepaling voor de implementatie en handhaving van de oorspronkelijke richtlijn van 2002. (Zie: B. VAN DER SLOOT en F.J. ZUIDERVEEN BORGESTUS, 'De amendementen van de Richtlijn Burgerrechten op de e-Privacyrichtlijn', *P & I* 2010/4, 162.)

[82] D. VOORHOOF en P. VALCKE (m.m.v. H. CANNIE), *Handboek Mediarecht (3de editie)*, Brussel, Larcier, 2011, 379.

eerbiediging van zijn privéleven en zijn gezinsleven, behoudens in de gevallen en onder de voorwaarden door de wet bepaald.

Het artikel valt inhoudelijk ongeveer te vergelijken met artikel 8 EVRM, maar er worden andere voorwaarden gesteld aan een eventuele inmenging in het recht op privacy dan wat vereist wordt in bovenvermelde 'beperkingsclausule' van artikel 8 EVRM. Het tweede lid van artikel 22 GW vereist een formele wet voor een inmenging, maar de toegevoegde waarde daarvan t.o.v. van artikel 8 EVRM is beperkt.[83] Artikel 8 EVRM biedt immers een additionele en meer solide bescherming bovenop de Belgische grondwetsbepalingen aangezien de bepalingen uit het EVRM directe werking hebben.

4.2 Belgische privacywetgeving

34. Het Dataprotectieverdrag van de Raad van Europa van 1981[84] is de aanzet geweest voor de uitvaardiging van de Wet Bescherming Persoonlijke levenssfeer (WBP) of Privacywet[85] van 1992.

België heeft de RBP omgezet in een wet van 11 december 1998 die de oude Privacywet grondig heeft gewijzigd.[86] Voor het toepassingsgebied en de principes bij de verwerking van persoonsgegevens kan worden verwezen naar de bespreking van de RBP (randnummers 26-31). De wet bevat net zoals de RBP geen specifieke bepalingen ter bescherming van de privacy van minderjarigen. Wel wordt, i.t.t. in de richtlijn, de zinsnede 'of zijn wettelijke vertegenwoordiger' toegevoegd aan de definitie van 'toestemming van de betrokkene' in artikel 1, §8 van de WBP.

5. De Amerikaanse COPPA

35. Zoals reeds aangegeven in de inleiding is het voor deze masterproef interessant te weten hoe men het probleem van de bescherming van de online privacy van kinderen heeft aangepakt in de Verenigde Staten. Een eerste opmerkelijk verschil met het Europese continent is alvast dat er in de V.S. specifieke wetgeving voorhanden is. In 1998 werd er de 'Children's Online Privacy Protection Act' (verder: COPPA) gestemd.[87]

---

[83] L. DIERICKX, *Het recht op afbeelding*, Antwerpen, Intersentia, 2005, 4.
[84] Zie voetnoot 76.
[85] Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, *BS*, 18 maart 1993.
[86] J. DUMORTIER, 'Privacybescherming bij de verwerking van persoonsgegevens', in X. (ed.), *Mediarecht, Telecommunicatie en telematica*, Mechelen, Kluwer, 1999, Afl. 12, 59-62.
[87] De COPPA is te raadplegen op: http://www.ftc.gov/ogc/coppa1.htm. Men dient deze wet te onderscheiden van de COPA (voluit: Child Online Protection Act). Deze laatste wet werd in het zelfde jaar gestemd als de COPPA, maar was gericht op de bescherming van minderjarigen tegen schadelijke inhoud op internet. De COPA werd ongrondwettelijk bevonden door het Supreme Court wegens schending van het recht op vrije meningsuiting waardoor de wet werd opgeschort. (ACLU v. Mukasey, 22 juli 2008, te raadplegen op: http://epic.org/free_speech/ copa/ACLU v Mukasey.pdf)

5.1 Ratio en achtergrond

36. Net als op het Europese continent zorgde de opkomst in de jaren negentig van de elektronische handel op het internet voor potentieel misbruik van persoonlijke informatie van consumenten door beheerders van websites. Met de COPPA trachtte de Amerikaanse wetgever het hoofd te bieden aan de specifieke risico's voor de privacy en veiligheid van kinderen.[88] Zo valt in het rapport van de Federal Trade Commission (FTC) het volgende te lezen: 'children's status as a special, vulnerable group is premised on the belief that children lack the analytical abilities and judgment of adults. […] In the specific arenas of marketing and privacy rights, moreover, several federal statutes and regulations recognize both the need for heightened protections for children and the special role that parents play in implementing these protections.'[89]

In 1998 werd door de Amerikaanse Federal Trade Commission (FTC) een onderzoek uitgevoerd naar de verwerking van de persoonsgegevens op internet. Van de 212 websites die zich specifiek richtten tot kinderen verwerkte 89% rechtstreeks persoonsgegevens van kinderen, maar vroeg slechts 23% hiervoor toestemming aan de ouders.[90] Op 21 oktober van hetzelfde jaar werd daarom in het Amerikaanse Congres een wetsvoorstel ingediend waarin de vier volgende doelstellingen werden aangegeven: (1) het stimuleren van de ouders om meer betrokken te zijn bij de online activiteiten van hun kinderen ten einde hun privacy op internet te beschermen, (2) het helpen beschermen van kinderen in online omgevingen zoals chat rooms en 'pen-pal' diensten waarbij kinderen informatie zouden kunnen vrijgeven, (3) de veiligheid garanderen bij het vergaren van de persoonsgegevens van kinderen op het internet en (4) vermijden dat persoonlijke informatie van kinderen wordt verzameld en verwerkt zonder ouderlijke toestemming.[91]

5.2 Toepassingsgebied

37. Aan de FTC werd de opdracht gegeven binnen het jaar regels uit te werken.[92] Deze Children's Online Privacy Protection Rule (verder: COPPR[93]), van kracht geworden op 21 april 2000, dicteert een aantal privacystandaarden voor websites die gericht zijn naar kinderen onder de dertien jaar. Bovendien schrijft de COPPR een meldingsplicht voor over de aard en het gebruik van de

[88] L. A. MATECKI, 'Update: COPPA is Ineffective Legislation! Next Steps for Protecting Youth Privacy Rights in the Social Networking Era', 5 Northwestern Journal of Law and Social Policy 2010, 369 en 373. (Hierna: L. A. MATECKI, 'COPPA Ineffective Legislation')
[89] FTC, Privacy Online: A Report to Congress (1998), te raadplegen op: http://www.ftc.gov/reports/ privacy/privacy5.shtm.
[90] Privacy Paper Cyberkids, *supra* noot 7, 42.
[91] A. FRACKMAN, R. C. MARTIN en C. RAY, *Internet and Online Privacy: A Legal and Business Guide*, ALM Publishing, 2002, 46 en L. A. MATECKI, 'COPPA Ineffective Legislation', *supra* noot 85, 375-376.
[92] Sectie 1303, (b) van de COPPA.
[93] De COPPR is te raadplegen op: http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&tpl=/ecfrbrowse/Title16/16cfr312_main_02.tpl

verzamelde informatie en verplicht het websites om ouderlijke toestemming te bekomen vooraleer de persoonlijke informatie van kinderen wordt opgeslagen.[94]

38. Een belangrijk verschil met de Europese visie in de RBP is dat de Amerikaanse wet werd uitgevaardigd specifiek ter bescherming van minderjarigen, meer bepaald voor kinderen onder de dertien jaar.[95] Volgens het rapport van de FTC kunnen minderjarigen boven de dertien immers bescherming vinden onder de 'Federal Trade Commission Act' van 1961. Jongeren tussen de dertien en zeventien jaar vallen aldus buiten het toepassingsgebied. In het rapport maakt men zelfs een onderscheid tussen kinderen onder en kinderen boven de twaalf jaar vanuit de redenering dat kinderen onder de twaalf jaar nog kwetsbaarder zijn en een striktere en meer verregaande privacybescherming behoeven dan de andere leeftijdsgroep.[96]

39. De verplichtingen die de COPPA voorschrijft zijn van toepassing op elke commerciële website of online dienstverlening die zich richt op kinderen onder de dertien jaar. SNS die zich richten tot kinderen onder die leeftijd vallen aldus onder de toepassing van de wet. De wet is tevens van toepassing op andere websites van zodra de operator weet ('has actual knowledge') dat hij gegevens van deze kinderen verzamelt.[97] 'Personal information' wordt gedefinieerd als 'individually identifiable information about an individual, including (A) a first and last name, (B) a home or other physical address including street name and name of a city or town, (C) an e-mail adress, (D) a telephone number, (E) a Social Security number, (F) any other identifier that the Commission determines permits the physical or online contacting of a specific individual or (G) information concerning the child or the parents of that child that the website collects online from the child and combines with an identifier described in this paragraph'. Op die manier is de COPPA niet alleen van toepassing op elke individueel identificeerbare informatie zoals contactgegevens maar ook op alle andere informatie die wordt verzameld d.m.v. bijvoorbeeld een cookie die men kan linken aan een bepaald identificeerbaar individu.[98]

5.3 Verplichtingen voor de beheerders van websites

40. Sectie 1303 van de COPPA (uitgewerkt in §312.4 van de COPPR) voorziet vooreerst een meldingsplicht ('notice'). De beheerders moeten op een duidelijke en opvallende wijze zowel op de homepage als op iedere webpagina waarop persoonsgegevens worden opgevraagd, links voorzien naar de privacy statement. Deze statement moet eenvoudig geformuleerd zijn en moet voldoen aan een aantal minimumvereisten.

Zeer belangrijk is de plicht voor de beheerders om verifieerbare of controleerbare ouderlijke toestemming te verkrijgen wanneer men gegevens van kinderen onder

[94] Zie Sectie 1303, (b), (1) onder (A) van de COPPA en Part 312 van de COPPR.
[95] Sectie 1302, (1) van de COPPA. De nieuwe Europese ontwerpverordening gegevensbescherming incorporeert echter wel de leeftijdsgrens van dertien jaar (zie randnummer 61).
[96] L. A. MATECKI, 'COPPA Ineffective Legislation', *supra* noot 85, 375.
[97] Privacy Paper Cyberkids, *supra* noot 7, 42.
[98] Privacy Paper Cyberkids, *supra* noot 7, 43.

de dertien jaar verwerkt. In het licht van de beschikbare technologie voorziet de COPPA hiervoor gradaties (de zgn. 'sliding scale' uitgewerkt in §312.5 van de COPPR) waarbij specifieke situaties al dan niet striktere formaliteiten behoeven voor het verkrijgen van de toestemming. Zo kan ouderlijke toestemming via e-mail volstaan indien de gegevens louter voor intern gebruik verzameld worden en niet beschikbaar zijn voor derden. Wanneer de persoonlijke informatie echter wordt meegedeeld of kan worden meegedeeld aan derden dan is een striktere voorwaarde vereist zoals een schriftelijke en ondertekende toestemming.

Verder voorziet de COPPA nog het recht van inzage door ouders in de door de beheerder vergaarde persoonlijke informatie van hun kind, het recht tot verbetering en verwijdering van de informatie en een aantal formele bepalingen.[99]

5.4 SNS en de Amerikaanse COPPA

5.4.1 Handhaving en de opkomst van SNS

41. Op Amerikaanse federaal niveau wordt een schending van de COPPA beschouwd als een 'unfair or deceptive trade practice' op grond van §5 van de Federal Trade Commission Act. De boetes kunnen oplopen tot 11 000 Amerikaanse dollar per inbreuk.[100] Drie jaar na het uitvaardigen van de wet legde de FTC zijn eerste boete op. Drie websitebeheerders, die gezamenlijk een site ter beschikking stelden die gericht was op meisjes tussen negen en veertien jaar, werden veroordeeld omdat ze niet voldeden aan de meldingsplicht en daarenboven informatie verzamelden van de jonge meisjes zonder de vereiste ouderlijke toestemming.[101] De eerste jaren na 1998 werd de COPPA aanzien als een succes en bleef grotendeels gespaard van kritiek.

42. Toen de FTC in 2006 voor de eerste maal een vordering instelde tegen een SNS trad de schaduwzijde van de wet op de voorgrond. Niet enkel een website die de leeftijd van de gebruikers niet controleerde of verifieerde via ouderlijke toestemming werd aansprakelijk geacht (*in casu* de SNS 'Xanga'), ook een website die voorzag in een toestemmingsmechanisme via e-mail (*in casu* 'Imbee') werd in 2008 toch veroordeeld door de FTC.[102] Het werd met de opkomst van de SNS alsmaar duidelijker dat het voor beheerders niet makkelijk is te voldoen aan de vage maar niettemin strenge COPPA-bepalingen. Zo maken de bewoordingen van een website 'directed towards children'[103] het lastig om te weten wanneer zij onder de toepassing van de wet vallen.

---

[99] Sectie 1303 van de COPPA, §312.6-12 van de COPPR en Privacy Paper Cyberkids, *supra* noot 7, 43-44.
[100] http://epic.org/privacy/kids/.
[101] L. A. MATECKI, 'COPPA Ineffective Legislation', *supra* noot 85, 379-380.
[102] L. A. MATECKI, 'COPPA Ineffective Legislation', *supra* noot 85, 381-382. De SNS 'Imbee' bleef de gegevens van kinderen verwerken ook al antwoordde de betreffende ouder niet op de toestemmingsemail. Op grond van § 312.8 van de COPPR moet de beheerder immers een betrouwbaar leeftijdsverificatiesysteem instellen. 'Imbee' moest een geldboete van 130 000 Dollar ophoesten.
[103] Sectie 1302, (10) van de COPPA en §312.2, laatste alinea van de COPPR.

De methodes voor leeftijdsverificatie die de FTC heeft vooropgesteld in de COPPR zoals het doorsturen van de kredietkaartcode van de ouders of het invullen van een digitaal formulier zijn volgens critici te kostelijk, hinderlijk en vooral oubollig geworden om op een efficiënte wijze persoonlijke informatie van kinderen af te schermen.[104] Bovendien lijkt de 'sliding scale' van §312.5 van de COPPR niet meer te voldoen aan de huidige technologische ontwikkelingen zodat alleen e-mail als het enige geschikte middel overblijft om ouderlijke toestemming te verkrijgen.[105] Beheerders trachten dan maar aan de wettelijke vereisten te voldoen door middel van 'age-screening'-systemen om gebruikers onder de dertien jaar te verbieden de website te betreden. In de realiteit kunnen kinderen deze restricties gemakkelijk omzeilen waardoor persoonlijke informatie toch wordt vrijgegeven en bijgevolg wordt verwerkt door beheerders die ogenschijnlijk handelen in overeenstemming met de wet.[106]

43. Aanvankelijk leek de FTC de ernstige 'drawbacks' van de COPPA sinds de opkomst van de SNS in de wind te slaan. In haar rapport van 2007 erkende de commissie uiteindelijk een aantal tekortkomingen van de wet w.o. de vage bewoordingen van websites 'directed to children' en het gebrek aan efficiënte technologische systemen voor leeftijdsverificatie. Toch achtte de FTC het niet nodig de COPPA te wijzigen. De commissieleden zagen 'consumer and business education' als een belangrijk aanvullend initiatief op de handhavingstaak van de commissie. De FTC mag dan iets te optimistisch zijn en een aantal ernstige wettelijke tekortkomingen klaarblijkelijk negeren, in 2007 onderkende het expliciet de uitdagingen van de nieuwe sociale media: 'still, the emergence of social networking sites, and other general audience sites that are attractive to teens, without the concomitant development of suitable age-verification technologies, presents challenges to website operators and parents, as well as the Commission.[107]

5.4.2 Een nieuwe COPPA?

44. De huidige COPPA ondergaat sinds de opkomst van de nieuwe sociale media hetzelfde lot als de Europese RBP en lag een aantal jaren na de uitvaardiging van de wet al hevig onder vuur. Verschillende consumenten- en privacygroepen hebben zich in 2008 gewend tot de FTC en voorstellen gedaan tot wijziging van de verouderde regelgeving.[108] Sommige critici pleiten voor een volledige eliminatie van de leeftijdsgrens van dertien jaar en van de ouderlijke toestemmingsvereiste opdat de last volledig op de schouders van websitebeheerders zou kunnen worden gelegd. Deze laatsten zouden dan verplicht zijn toestemming te vragen aan de (minderjarige) gebruiker zelf. Anderen zijn dan weer voorstander van verplichte 'opt-in'-systemen waarbij

[104] http://epic.org/privacy/kids/.
[105] L. A. MATECKI, 'COPPA Ineffective Legislation', *supra* noot 85, 386-387.
[106] L. A. MATECKI, 'COPPA Ineffective Legislation', *supra* noot 85, 386-387.
[107] FTC, Implementing the Children's Online Privacy Protection Act: A Report to Congress, februari 2007. Te raadplegen op: http://www.ftc.gov/oia/ftccoppareport.pdf.
[108] L. A. MATECKI, 'COPPA Ineffective Legislation', *supra* noot 85, 397.

persoonlijke informatie maar kan vrijgegeven worden wanneer de gebruiker uitdrukkelijk zijn toestemming geeft.[109]

45. MATECKI onderscheidt drie belangrijke wijzigingen die de wetgever in acht zou moeten nemen teneinde jonge gebruikers in staat te stellen geïnformeerde keuzes te maken omtrent hun online privacyrechten. Ten eerste zou het toepassingsgebied van de wet uitgebreid moeten worden naar jongeren (minderjarigen ouder dan dertien jaar). De huidige leeftijdsgrens van dertien jaar wordt in de realiteit vertaald in online leeftijdsrestricties die kinderen probleemloos kunnen omzeilen. Procentueel zijn er meer jongeren aangesloten op SNS dan jonge kinderen. Bovendien zijn tieners vaak nog kwetsbaarder voor miskenning van hun privacy dan kinderen door de 'peer pressure' op SNS.[110]

Ten tweede pleit de auteur voor beperkte 'opt-in'-vereisten die verschillend zijn voor jongeren en kinderen. Zo zouden verplichte 'opt-in'-bepalingen van toepassing zijn voor kinderen onder de dertien jaar teneinde adverteerders te verhinderen persoonlijke informatie van jonge kinderen in handen te krijgen. Jongeren ouder dan dertien jaar en meerderjarigen zouden 'opt-out'-instellingen hebben die naargelang de leeftijd de doorgang van gegevens bemoeilijken of vergemakkelijken. Hierbij dient een evenwicht te worden gezocht tussen de belangen van websitebeheerders en adverteerders en de privacybescherming van kinderen en jongeren.[111]

Ten slotte zouden volgens de auteur de meldings- en toestemmingsvoorwaarde moeten worden verscherpt. De systemen en technieken die de FTC voorziet voor ouderlijke toestemming zijn lang niet meer aangepast aan de huidige online problematiek. Eveneens zou hier een zwaardere last op de schouders van beheerders moeten worden gelegd in plaats van deze taak aan de ouders toe te wijzen. Een aangepast en creatief verificatiesysteem zou gericht moeten worden naar de jonge gebruikers zelf teneinde kinderen en jongeren te informeren en bewust te maken van de online privacyrisico's.[112]

6. SNS in het licht van de Europese gegevensbeschermingswetgeving

46. In Europa vallen sociale netwerkdiensten onder het toepassingsgebied van de EU-wetgeving betreffende de gegevensbescherming, zijnde de RBP en in de toekomst waarschijnlijk de gegevensbeschermingsverordening. In het pre-internettijdperk van de jaren negentig, gekenmerkt door het gebruik van netwerken met een gecentraliseerde en lokale gegevensverwerking, was het bestaande regelgevend kader van dataprotectie nog relatief eenvoudig toe te passen. Door de enorme toename aan gegevensverzameling met de opkomst

[109] L. A. MATECKI, 'COPPA Ineffective Legislation', *supra* noot 85, 397-398.
[110] L. A. MATECKI, 'COPPA Ineffective Legislation', *supra* noot 85, 399-400.
[111] L. A. MATECKI, 'COPPA Ineffective Legislation', *supra* noot 85, 400.
[112] L. A. MATECKI, 'COPPA Ineffective Legislation', *supra* noot 85, 401-402. 'These creative solutions would foster 'maximum possibile comprehension' of users' rights, and ensure proper notice and consent to usage terms among all users, but especially the vulnerable children and teen demographics', aldus de auteur.

van Web 2.0.-tendensen is het bijzonder relevant na te gaan in hoeverre en onder welke voorwaarden de RBP kan worden toegepast op de context van SNS.

6.1 Profielgegevens

47. Profielgegevens op een SNS hebben betrekking, zij het direct of indirect, op een geïdentificeerde of identificeerbare natuurlijke persoon en kunnen gekwalificeerd worden als een 'persoonsgegeven' in de zin van artikel 2, a) van de RBP.[113] Het nieuwe voorstel tot verordening (zie randnummers 59-72) voorziet echter een scherpere definitie zodat een online profiel nu ongetwijfeld onder de toepassing van de gegevensbeschermingsregels zal vallen: 'iedere informatie betreffende een geïdentificeerde natuurlijke persoon of een natuurlijke persoon die direct of indirect, met behulp van middelen waarvan mag worden aangenomen dat zij redelijkerwijs door de voor de verwerking verantwoordelijke dan wel door een andere natuurlijke of rechtspersoon in te zetten zijn, kan worden geïdentificeerd, met name aan de hand van een identificatienummer, gegevens over de verblijfplaats, *een online-identificatiemiddel* of een of meer specifieke elementen die kenmerkend zijn voor zijn fysieke, fysiologische, genetische, mentale, economische, culturele of sociale identiteit'.[114]

6.2 Aanbieders van sociale netwerkdiensten en gebruikers

48. De WG 29 stelt in haar advies 5/2009 over online sociale netwerken dat de RBP in de meeste gevallen van toepassing is op aanbieders van sociale netwerkdiensten, ook als hun hoofdkantoor buiten de EER is gelegen.[115] In dat geval kunnen de aanbieders gekwalificeerd worden als 'voor de verwerking verantwoordelijken'. Het zijn immers zij die de middelen verstrekken voor de verwerking van de gebruikersgegevens en diensten aanbieden zoals het openen en het verwijderen van accounts.

49. Het strikte onderscheid tussen de verantwoordelijke voor de verwerking en de verwerker als eenvoudige uitvoerder dat in de RBP wordt gebezigd, weerspiegelt de tijdsgeest waarin het internet en gegevensverwerking nog hoofdzakelijk gebaseerd waren op de centrale vergaring van gegevens door een beperkt aantal spelers. Tegenwoordig worden gegevens verwerkt door een ontelbaar aantal belanghebbenden waardoor deze binaire opdeling aanzienlijke rechtsonzekerheid teweeg kan brengen. Zeker in de context van SNS komt dit onderscheid kunstmatig over aangezien zowel de aanbieder van sociale netwerkdiensten als de gebruikers gekwalificeerd kunnen worden als verantwoordelijke en/of als verwerker.[116]

Over deze rechtsonzekere kwalificatie vaardigde de WG 29 begin 2010 een advies uit om meer duidelijkheid te scheppen over het onderscheid tussen verant-

[113] P. VAN EECKE en M. TRUYENS, 'Privacy en sociale netwerken', *supra* noot 8, 122.
[114] Artikel 4, 1) en 2) van de ontwerpverordening. Zie ook: 'Nieuwe privacyregels voor sociale netwerken', 9 maart 2012, http://www.wisemen.nl/weblog/weblogs/nieuwe-europese-privacyregels-relevant-voor-sociale-netwerken/.
[115] WG 29, Advies 5/2009, *supra* noot 39.
[116] P. VAN EECKE en M. TRUYENS, 'Privacy en sociale netwerken', *supra* noot 8, 117.

woordelijken en verwerkers in het licht van de huidige internetomgeving.[117] Aan de hand van voorbeelden tracht de werkgroep de verenigbaarheid met de huidige wetgeving aan te tonen en benadrukt het belang van de gezamenlijke verantwoordelijkheid. Vertaald in de context van SNS wordt bevestigd dat zowel de beheerder als de gebruiker gekwalificeerd worden als gezamenlijke verantwoordelijken voor de verwerking van accountgegevens van de gebruiker en persoonsgegevens van derden. Het advies lijkt veeleer een manier te zijn om te benadrukken dat het huidige regelgevend kader nog steeds in staat is om het hoofd te bieden aan de hedendaagse informatiestroom van gegevens. Anno 2012 weten we wel beter.

6.3 De vrijstelling voor persoonlijke of huishoudelijke doeleinden

50. In artikel 3, §2, 2de streepje van de RBP is een zgn. vrijstelling voor persoonlijke of huishoudelijke doeleinden voorzien: de verwerking van persoonsgegevens 'die door een natuurlijk persoon in activiteiten *met uitsluitend persoonlijke of huishoudelijke doeleinden* wordt verricht' valt buiten de toepassing van de richtlijn. Deze uitzondering is er om te voorkomen dat alledaagse handelingen van privépersonen, zoals het bijhouden van een adresboekje, onder de werking van de privacyregelgeving zou vallen. Deze opvatting is door de toenemende digitalisering en online evolutie intussen voorbijgestreefd. Nu kan immers door iedereen enorme hoeveelheden gevoelige informatie worden bijgehouden door de aanzienlijke opslagcapaciteit van numerieke dragers en de connectiviteit van hedendaagse computers.[118]

6.3.1 De zaak Lindqvist

51. Een belangrijke beslissing van het Hof van Justitie in het licht van de verwerking van persoonsgegevens op internet is de zaak Lindqvist van 2003.[119] Mevrouw Bodil Lindqvist was een Zweedse godsdienstlerares die een website had opgezet voor de kerkgemeenschap waarvan zij deel uitmaakte. Zonder voorafgaande toestemming plaatste ze informatie over haar collega's van de kerkgemeenschap op haar homepage, w.o. hun naam, gezinssituatie en telefoonnummers. Verder vermeldde ze dat één van haar collega's haar voet had bezeerd en met gedeeltelijk ziekteverlof was. Mevrouw Lindqvist werd door de Zweedse rechter veroordeeld tot betaling van een geldboete van 4000 SEK (ongeveer 450 euro) en stelde hoger beroep in bij het Göta Hovrätt.[120] De Zweedse appelrechter stelde een aantal prejudiciële vragen aan het Hof van Justitie waarvan de volgende de belangrijkste zijn: 'is het vermelden van een persoon, met naam of met naam en telefoonnummer, op een homepage op het internet een handeling die onder de werkingssfeer van richtlijn 95/46 valt?' en is

---

[117] Werkgroep Gegevensbescherming Artikel 29, Advies 1/2010 over de begrippen 'voor de verwerking verantwoordelijke' en 'verwerker', 16 februari 2010. Te raadplegen op: http://ec.europa.eu/justice/ policies/privacy/docs/wpdocs/2010/wp169_nl.pdf. (Hierna: WG 29, Advies 1/2010)

[118] P. VAN EECKE en M. TRUYENS, 'Privacy en sociale netwerken', *supra* noot 8, 120.

[119] HvJ, 6 november 2003 (C-101/01), *Jur.* I-12971.

[120] P. VAN EECKE en M. TRUYENS, 'Privacy en sociale netwerken', *supra* noot 8, 120.

er sprake van een 'geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens wanneer op een eigenhandig gecreëerde homepage op het internet een aantal personen worden vermeld met verklaringen en mededelingen omtrent onder meer hun werksituatie of hobby?'. [121]

Het Hof van Justitie oordeelde in 2003 dat op de activiteiten van Mevrouw Lindqvist de RBP van toepassing is en kwalificeerde de activiteiten op de website als een verwerking van persoonsgegevens. De vermelding van het feit dat iemand zijn voet heeft bezeerd en met gedeeltelijk ziekteverlof is, is volgens het Hof een persoonsgegeven betreffende de gezondheid in de zin van artikel 8, lid 1 RBP. Naar de geest van de richtlijn is de door het Hof gemaakte kwalificatie als verwerking van persoonsgegevens echter voor kritiek vatbaar. Het kan immers niet de bedoeling zijn om iemand die wetenswaardigheden over anderen op een internetsite plaatst te verplichten het doel van de verwerking te specifiëren en de verwerking aan te melden conform de RBP.[122]

Het Hof besliste dat in de situatie van Mevrouw Lindqvist de vrijstelling van artikel 3, § 2, 2de streepje niet kon worden ingeroepen aangezien genoemde uitzondering uitsluitend betrekking moet hebben op activiteiten die tot het persoonlijke of gezinsleven van particulieren behoren. Bovendien moet bij het plaatsen van persoonsgegevens op het internet de informatie voor een onbepaald aantal personen toegankelijk zijn. Vrijwilligerswerk of religieuze activiteiten zijn immers niet gelijk te stellen met de activiteiten vermeld in de uitzonderingsbepaling.[123]

Belangrijk voor sociale netwerkdiensten is dat het Hof hier beslist dat indien persoonsgegevens voor een onbepaald aantal personen toegankelijk wordt gemaakt op een website, de vrijstelling niet van toepassing is. Over de wijze waarop het concept van persoonlijke of huishoudelijke activiteiten inhoudelijk moet worden ingevuld, rept het Hof daarentegen geen woord.[124]

6.3.2 De SNS-gebruiker en de vrijstelling

52. Voor SNS-gebruikers zou de vrijstelling betekenen dat personen die voor puur persoonlijke of huishoudelijke doeleinden informatie meedelen op SNS zich kunnen beroepen op de wettelijke uitzondering opdat hun activiteiten niet onder de RBP zouden vallen. De WG 29 merkt op dat het in bepaalde omstandigheden kan voorkomen dat de activiteiten van de SNS-gebruiker niet onder de vrijstelling vallen en de gebruiker geacht wordt bepaalde verantwoordelijkheden van een voor de verwerking verantwoordelijke op zich te hebben genomen.[125] Wanneer een gebruiker aldus optreedt namens een bedrijf of organisatie of diensten gebruikt voor commerciële, politieke of charitatieve doeleinden, zal hij zich niet kunnen beroepen op de vrijstelling en zal de richtlijn van toepassing zijn op de verwerking van de gegevens. Opmerkelijk is dat volgens de werkgroep een

[121] HvJ, 6 november 2003 (C-101/01), *Jur.* I-12971, punt 18.
[122] A.R. LODDER e.a., 'Recht en Web 2.0.', *supra* noot 43, 121.
[123] HvJ, 6 november 2003 (C-101/01), *Jur.* I-12971, punten 27, 38, 43-48.
[124] P. VAN EECKE en M. TRUYENS, 'Privacy en sociale netwerken', *supra* noot 8, 120.
[125] WG 29, Advies 1/2010, *supra* noot 114, 6.

groot aantal contactpersonen een aanwijzing kan zijn dat de vrijstelling niet geldt en de gebruiker zal kwalificeren als een 'voor de verwerking verantwoordelijke'.

Volgens de WG 29 wordt aldus in de meeste gevallen een gebruiker beschouwd als een 'betrokkene', maar in sommige omstandigheden kan het zijn dat de gebruiker geacht wordt een voor de verwerking verantwoordelijke te zijn en de bijbehorende plichten op grond van de privacyregelgeving evenzeer naar hem gericht zijn. De structuur en de technologie die wordt gebruikt voor de verwerking worden alleen door de beheerder van het netwerk bepaald, maar de gebruiker bepaalt ook zelf het doel en de middelen van de verwerking door te kiezen op welke SNS hij een profiel wil aanmaken, welke applicaties hij daarbij selecteert en voor welke doeleinden hij zijn netwerk zal gebruiken.[126] Indien de gebruiker gegevens over derden zoals foto's en video's beschikbaar stelt op een SNS treedt hij op als verantwoordelijke voor de verwerking terwijl in dit geval de beheerder zal optreden als de verwerker.

Interessant in dit opzicht is dat de werkgroep tevens verduidelijkt dat in het geval dat de profielinformatie ook toegankelijk is voor anderen dan de door de gebruiker gekozen contactpersonen, de gebruiker zich ook niet zal kunnen beroepen op de vrijstelling. Dit zal het geval zijn wanneer bijvoorbeeld het profiel van de gebruiker toegankelijk is voor alle leden van een sociale netwerkdienst, de gegevens ook geïndexeerd kunnen worden door zoekmachines of wanneer kan worden vastgesteld dat bij het aanvaarden van contactpersonen geen werkelijke keuze wordt gemaakt, bijvoorbeeld wanneer gebruikers contactpersonen aanvaarden ongeacht de relatie die tussen hen bestaat.[127] Terecht merken VAN EECKE en TRUYENS op dat aan de hand van deze door de werkgroep vooropgestelde criteria er in realiteit juist zeer veel gebruikers van SNS buiten de toepassing van de vrijstelling zullen vallen en aldus zullen kwalificeren als verantwoordelijken voor de verwerking.[128] De bewoordingen 'persoonlijke of huishoudelijke doeleinden' stroken dus niet meer met de Web 2.0-realiteit en het Hof van Justitie zou zich in de toekomst moeten uitspreken over de vraag wat deze bewoordingen inhoudelijk betekenen in het licht van de huidige SNS-constellatie.

6.4 Aanbieders van applicaties

53. Belangrijk om op te merken is dat aanbieders van applicaties op een SNS eveneens gekwalificeerd kunnen worden als 'voor de verwerking verantwoordelijken'. In dat geval wordt de aanbieder van het sociale netwerk beschouwd als een loutere verwerker. Als voorwaarde hiervoor bepaalt de WG 29 dat de applicaties als aanvulling op de applicaties van de sociale netwerkdienst moeten functioneren en dat de gebruikers besluiten een dergelijke applicatie te gebruiken.[129] Omdat deze aanbieders meestal ook toegang hebben tot de informatie die door de gebruiker wordt opgeslagen en de beheerders deze

[126] P. VAN EECKE en M. TRUYENS, 'Privacy en sociale netwerken', *supra* noot 8, 118.
[127] WG 29, Advies 1/2010, *supra* noot 114, 7.
[128] P. VAN EECKE en M. TRUYENS, 'Privacy en sociale netwerken', *supra* noot 8, 121.
[129] WG 29, Advies 1/2010, *supra* noot 114, 6.

aanbieders beschouwen als loutere derden leidt deze verwevenheid tot een gebrek aan transparantie en vooral voor de gebruiker tot een gebrek aan rechtszekerheid.[130]

6.5 De plichten van de voor de verwerking verantwoordelijke

54. Indien de aanbieder van de sociale netwerkdienst en/of de gebruiker gekwalificeerd worden als verantwoordelijke voor de verwerking, bevat de RBP belangrijke verplichtingen die in de context van SNS een aantal moeilijkheden met zich kunnen meebrengen.

Op grond van artikel 6, 1ste lid, e) van de RBP mogen de persoonsgegevens, in een vorm die het mogelijk maakt de betrokkenen te identificeren, niet langer worden bewaard dan voor de verwezenlijking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, noodzakelijk is (zie ook randnummer 29). De aanbieder van SNS dient de persoonsgegevens van een gebruiker te wissen van zodra deze laatste of de sociale netwerkdienst zelf het account opzegt. Informatie die door de gebruiker wordt gewist, mag in beginsel niet worden bewaard. In de praktijk weten we dat het volledig verwijderen van een opgebouwd sociaal netwerkprofiel geen sinecure is. De persoonsgegevens worden vaak nog een tijdje bewaard na de schrapping van het account. Volgens VAN EECKE en TRUYENS zou er tussen de schrapping en de effectieve verwijdering van de gegevens geen lange tijdsperiode mogen verlopen.[131] Deze grijze zone zou met de bijzondere bepaling betreffende het zgn. 'recht om vergeten te worden' in de nieuwe ontwerptekst worden opgehelderd (zie randnummer 65).

Artikel 10 van de RBP schrijft een informatieplicht voor waarbij de verantwoordelijke de gebruikers moet informeren over de identiteit van de aanbieder en de verschillende doeleinden waarvoor de persoonsgegevens worden verwerkt (zie randnummer 29). Zo dienen gebruikers door de aanbieders gewezen te worden op de privacyrisico's en op het feit dat voor het plaatsen van afbeeldingen of informatie over anderen zij hiervoor de toestemming nodig hebben van de betrokkenen. SNS-aanbieders en aanbieders van applicaties kunnen hieraan voldoen door middel van een privacy statement en duidelijke vermeldingen op de SNS zelf. Gebruikers, te kwalificeren als verantwoordelijke voor de verwerking, moeten op hun beurt elkaar inlichten wanneer de betrokkene niet op de hoogte is van het plaatsen van bepaalde gegevens op een SNS.[132] Voor het plaatsen van gevoelige gegevens in de zin van artikel 8, lid 1 van de RBP[133] hebben sociale netwerkdiensten en gebruikers eveneens de uitdrukkelijke toestemming van de betrokkene nodig.

Artikel 18 van de RBP schrijft een meldingsplicht voor. De voor de verwerking verantwoordelijke moet voorafgaandelijk aangifte doen van de voorgenomen

[130] P. VAN EECKE en M. TRUYENS, 'Privacy en sociale netwerken', *supra* noot 8, 121.
[131] P. VAN EECKE en M. TRUYENS, 'Privacy en sociale netwerken', *supra* noot 8, 124.
[132] P. VAN EECKE en M. TRUYENS, 'Privacy en sociale netwerken', *supra* noot 8, 127.
[133] 'Persoonlijke gegevens waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging, of het lidmaatschap van een vakvereniging blijkt, alsook de verwerking van gegevens die de gezondheid of het seksuele leven betreffen.'

verwerking bij de nationale toezichthoudende autoriteit. Zowel SNS-aanbieders, aanbieders van applicaties als de gebruikers zijn in principe onderworpen aan deze verplichting. In de praktijk doet geen enkele SNS-gebruiker aangifte en is de toegevoegde waarde van deze regel in de context van SNS dan ook nihil.[134] De meldingsplicht wordt bovendien afgeschaft door de nieuwe ontwerpverordening.

Op grond van artikel 17 van de RBP moet de verantwoordelijke ten slotte passende technische en organisatorische maatregelen treffen om de veiligheid te waarborgen gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen. De aanbieder van sociale netwerkdiensten dient in dit opzicht standaardinstellingen te voorzien ter vrijwaring van de privacy van de gebruikers. Dit om te vermijden dat derden zomaar kunnen doorklikken naar persoonsgegevens op het profiel van de gebruiker.[135]

6.6 Rechten van de gebruikers

55. Zowel gebruikers als niet-gebruikers[136] van de SNS hebben het recht van toegang tot, rectificatie en uitwissing van de gegevens op grond van artikel 12 van de RBP.[137] Dus ook wanneer een derde een gebruiker verzoekt om onjuiste gegevens te corrigeren of te verwijderen dient daaraan gevolg gegeven te worden.

Op grond van artikel 14 heeft de betrokkene een recht van verzet, nl. het recht om 'zich […] te allen tijde om zwaarwegende en gerechtvaardigde redenen die verband houden met zijn bijzondere situatie ertegen te verzetten dat hem betreffende gegevens het voorwerp van een verwerking vormen, […].' Dit is echter niet evident wanneer de betrokkene reeds zijn uitdrukkelijke toestemming heeft gegeven, maar de gebruiker toch bepaalde gegevens zal moeten verwijderen wanneer de betrokkene dit eist op grond van zijn recht van verzet.[138]

56. Vermeldenswaardig is ten slotte de volgende richtsnoer van de WG 29: 'gebruikers moeten in het algemeen worden toegestaan gebruik te maken van een pseudoniem'.[139] Er is geen reden om de werkelijke naam van de gebruikers te plaatsen op het internet en SNS zouden gebruikers de keuze moeten laten. In het advies van 2012 over het voorstel voor een nieuwe verordening stelt de werkgroep voor om een algemene verplichting van 'pseudonimisatie' van persoonlijke informatie in te voeren waar dit haalbaar en proportioneel met het doel van de verwerking zou zijn.[140]

---

[134] P. VAN EECKE en M. TRUYENS, 'Privacy en sociale netwerken', *supra* noot 8, 125.
[135] WG 29, Advies 5/2009, *supra* noot 39.
[136] Niet-gebruikers zijn natuurlijke personen die geen lid zijn, maar van wie gegevens worden verwerkt, bijvoorbeeld wanneer iemands e-mailadres wordt gebruikt door de SNS.
[137] WG 29, Advies 5/2009, *supra* noot 39, 12.
[138] P. VAN EECKE en M. TRUYENS, 'Privacy en sociale netwerken', *supra* noot 8, 125.
[139] WG 29, Advies 5/2009, *supra* noot 39, 15.
[140] Article 29 Data Protection Working Party, Opinion 01/2012 on the data protection reform proposals, 23 march 2012, 11. Te raadplegen op: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf. (Hierna: WG 29, Advies 01/2012) (De tekst van het advies is voorlopig enkel in het Engels beschikbaar.)

HOOFDSTUK 2. MINDERJARIGEN, SNS EN HET VOORSTEL TOT ALGEMENE VERORDENING GEGEVENSBESCHERMING VAN 25 JANUARI 2012

Afdeling 1. Ratio en achtergrond van de ontwerpverordening

57. De verschillen in nationale implementatie van de RBP hebben geleid tot een zeer gefragmenteerd beleid binnen de EU. De oude richtlijn blijkt de snelle technologische en informationele ontwikkelingen niet meer te kunnen bijbenen.[141] Om deze redenen werd begin dit jaar een voorstel ingediend tot wijziging van de richtlijn.[142] De Europese Commissie legt de nieuwe regels vast in een voorstel tot verordening.[143] De regels zouden derhalve op grond van artikel 288 VWEU rechtstreeks toepasselijk zijn. Dit betekent dat de lidstaten het nieuwe kader niet hoeven om te zetten in nationaal recht. De regels betreffende gegevensbescherming gericht naar politie en justitie zijn echter vastgelegd in een voorstel tot richtlijn.[144]

De bedoeling van de wijziging van de bestaande regelgeving is volgens de Europese Commissie het tot stand brengen van een krachtiger en meer coherent kader voor gegevensbescherming in de EU en hierbij scherp toe te zien op de handhaving ervan (overweging 6).[145] Bovendien is de regelgeving bedoeld om de ontwikkeling van innovatieve toepassingen van nieuwe en complexe technologieën zoals 'cloud computing' niet in de weg te staan en tegelijkertijd meer rechtszekerheid en harmonisering te bewerkstelligen dan nu het geval is onder de RBP (overwegingen 5 en 7).[146]

58. De ontwerpverordening bevat een aantal belangrijke nieuwigheden. Zo is er vooreerst een uitbreiding van het territoriale toepassingsgebied in artikel 3 die tegemoet komt aan vroegere discussies over het toepasselijke recht in

---

[141] C. PRINS, 'Gelekte voorstellen EU wetgeving betreffende bescherming persoonsgegevens', *Computerr.* 2012/1, 89.

[142] Voorstel voor een verordening van het Europees Parlement en de Raad van 25 januari 2012 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (algemene verordening gegevensbescherming), COM(2012) 11 definitief, te raadplegen op: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_nl.pdf, 1-2. (Hierna: Voorstel algemene verordening gegevensbescherming) Het voorstel vindt zijn juridische grondslag in het nieuwe artikel 16 VWEU op grond waarvan voorschriften kunnen worden vastgesteld betreffende de bescherming van natuurlijke personen ten aanzien van de verwerking van persoonsgegevens door lidstaten bij de uitoefening van activiteiten die binnen het toepassingsgebied van het EU-recht vallen.

[143] Er werd sinds het Verdrag van Lissabon een nieuwe rechtsgrondslag ingevoerd voor de vaststelling van een coherent Europees wettelijk kader betreffende de bescherming van persoonsgegevens, nl. artikel 16 VWEU.

[144] Voorstel algemene verordening gegevensbescherming, *supra* noot 139, 6 en voorstel voor een richtlijn van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van strafrechtelijke sancties, en betreffende het vrije verkeer van die gegevens, COM(2012) 10 definitief.

[145] Voorstel algemene verordening gegevensbescherming, *supra* noot 139, 1-2.

[146] Zie ook: Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's, 'Een integrale aanpak van de bescherming van persoonsgegevens in de Europese Unie', 4.11.2010, COM(2010) 609 definitief.

internationale context. Voortaan zullen de regels van toepassing zijn op de verwerking van persoonsgegevens door alle voor de verwerking verantwoordelijken en verwerkers die gevestigd zijn in de EU ongeacht of de verwerking op zich in de EU plaatsvindt of niet. Bovendien zal de nieuwe verordening eveneens van toepassing zijn indien de voor de verwerking verantwoordelijke gegevens verwerkt van EU-onderdanen in het kader van het aanbieden van goederen of diensten aan de betrokken personen of met het doel hun gedrag te observeren, maar geen zetel heeft binnen de EU. [147] De ontwerpverordening wil het fenomeen van 'forum-shopping' vermijden. Bedrijven kunnen immers door het huidige gefragmenteerde beleid onder de RBP hun hoofdvestiging trachten te verplaatsen naar een lidstaat met de minst verregaande privacywetgeving en de meest incompetente toezichthouder. Onder de nieuwe regeling kunnen bedrijven voortaan terecht bij één nationale toezichthouder in het land waar ze hun Europese hoofdvestiging hebben (overweging 11).[148] Dit 'one-stop-shop'-systeem moet worden ingesteld door elke lidstaat op grond van de artikelen 46 en 49.

Tegenover de administratieve vereenvoudiging voor de ondernemingen staat wel dat zij meer verregaande verplichtingen hebben dan onder het oude regime en dat zij een hoog beschermingsniveau van de verzamelde gegevens moeten kunnen garanderen. Zo wordt bij de artikelen 30 en 31 de verplichting ingevoerd om inbreuken in verband met persoonsgegevens te melden.[149] De verordening voorziet daarenboven een effectiever sanctiemechanisme in hoofdstuk VIII. Het nieuwe kader poogt de verantwoordelijkheid van de voor de verwerking verantwoordelijken aldus te verhogen en de positie van de toezichtsautoriteiten te verstevigen.

Opvallend zijn de wijzigingen in artikel 5 van de ontwerptekst waarin wordt bepaald dat de persoonsgegevens verwerkt moeten worden 'op een wijze die rechtmatig, eerlijk *en transparant* is ten opzichte van de betrokkene'. I.t.t. artikel 6 RBP (zie randnummer 29) wordt op die manier expliciet een algemeen transparantiebeginsel geïntroduceerd. Nieuw zijn tevens de verduidelijking van het beginsel van minimale gegevensverwerking en de vaststelling van alomvattende verantwoordelijkheid en aansprakelijkheid van de voor de verwerking verantwoordelijke.[150]

Andere belangrijke nieuwigheden zijn het recht om gegevens over te dragen (artikel 18), het recht om vergeten te worden (artikel 17), het recht niet onderworpen te worden aan beslissingen gebaseerd op profielen (artikel 20) en het principe van 'privacy by default' (artikel 23). Deze bepalingen zijn uiterst belangrijk wat SNS betreffen en worden *infra* toegelicht (randnummers 59-72).

---

[147] Zie vooral: C. PRINS, 'Gelekte voorstellen EU wetgeving betreffende bescherming van persoonsgegevens', *Computerr.* 2012/1, 90 en S. VYNCKE, 'Het voorstel voor een Europese Privacy Verordening doorgelicht', http://siriuslegal.wordpress.com/2012/02/06/het-voorstel-voor-een-europese-privacy-verordening-doorgelicht/.

[148] C. PRINS, 'Gelekte voorstellen EU wetgeving betreffende bescherming persoonsgegevens', *Computerr.* 2012/1, 89.

[149] Voorstel algemene verordening gegevensbescherming, *supra* noot 139, 11.

[150] Voorstel algemene verordening gegevensbescherming, *supra* noot 139, 8.

Ten slotte zijn er nog een aantal formele en procedurele veranderingen. Zo wordt in artikel 33 een privacyeffectbeoordeling voorzien en wordt de WG 29 vervangen door een Europees Comité voor gegevensbescherming (artikel 64).

Afdeling 2. De nieuwe bepalingen in de ontwerptekst

59. Het gebrek aan bijzondere bepalingen op zowel Europees als nationaal niveau ter bescherming van de persoonlijke levenssfeer van minderjarigen heeft de Europese wetgever er toe gebracht een aantal wijzingen door te voeren in de bestaande regelgeving in het kader van het belang van het kind. Begin december 2011 was het voorstel reeds gelekt op internet.[151] Een interessante bemerking is dat in artikel 5 van de eerdere draftversie het belang van het kind uitdrukkelijk genoemd werd bij de afweging van het belang van de verantwoordelijke en de betrokkene bij de verwerking van de gegevens.[152] Deze bepaling is verdwenen in de definitieve ontwerptekst.

Het zou nogal ongeloofwaardig overkomen indien de Europese wetgever in de nieuwe verordening geen rekening zou houden met het fenomeen van sociale netwerkdiensten. Er zijn dan ook een aantal cruciale artikelen in de ontwerptekst die interessante gevolgen met zich mee brengen voor SNS. Dit betekent alvast dat de SNS-aanbieders hun bedrijfsvoering en beleid zullen moeten aanpassen aan deze nieuwe regels indien de ontwerptekst zal worden goedgekeurd.

1. Kinderen

60. Vooreerst zijn een aantal nieuwe definities opgenomen in artikel 4 van het voorstel w.o. de definitie van 'kind' als zijnde 'iedere persoon die jonger is dan achttien jaar'.[153] Overweging 29 verduidelijkt dat kinderen extra bescherming verdienen 'aangezien zij zich allicht minder bewust zijn van de risico's, gevolgen, beschermingsmaatregelen en rechten in verband met de verwerking van persoonsgegevens'.

61. Het voorstel voorziet een artikel 8 waarin de voorwaarden worden vastgelegd betreffende de rechtmatigheid van de verwerking van persoonsgegevens van kinderen in het kader van diensten van de informatiemaatschappij die hun rechtstreeks worden aangeboden. Het eerste lid van artikel 8 bepaalt dat de verwerking van persoonsgegevens van kinderen jonger dan dertien jaar (merk op dat dit dezelfde leeftijdsgrens is als in de Amerikaanse COPPA (zie randnummer 37)) bij het rechtstreeks aanbieden van diensten van de informatiemaatschappij slechts rechtmatig is 'wanneer en voor zover de ouder of voogd van het kind daartoe toestemming heeft gegeven of machtiging tot toestemming heeft verleend'. De voor de

---

[151] C. PRINS, 'Gelekte voorstellen EU wetgeving betreffende bescherming van persoonsgegevens', *Computerr.* 2012/1, 89.

[152] Bovendien werd voorzien dat het verwerken van persoonsgegevens voor 'direct marketing' voor commerciële doeleinden enkel wettig is indien de betrokkene zijn uitdrukkelijke toestemming heeft gegeven. Vooral dit laatste werd als te verregaand beschouwd en na lobbywerk van o.a. belangenorganisatie FEDMA is deze bepaling verdwenen uit de ontwerptekst. (Zie: C. PRINS, 'Gelekte voorstellen EU wetgeving betreffende bescherming van persoonsgegevens', *Computerr.* 2012/1, 90 en S. VYNCKE, 'Het voorstel voor een Europese Privacy Verordening doorgelicht', http://siriuslegal.wordpress.com/2012/02/06/het-voorstel-voor-een-europese-privacyverordening-doorgelicht/.)

[153] In overweging 29 wordt verduidelijkt dat de definitie in artikel 4, 18) gebaseerd is op de definitie uit het VN-Kinderrechtenverdrag (zie voetnoot 21).

verwerking verantwoordelijke dient hierbij met inachtneming van de beschikbare technologie verifieerbare toestemming te verkrijgen op een manier die 'redelijkerwijze van hem kan worden verwacht'.

2. Toestemming

62. Momenteel heerst op Europees niveau nogal wat rechtsonzekerheid over de toestemmingsvereiste in de huidige gegevensbeschermingsregelgeving in het licht van SNS. Bij het online registreren komt men meestal niet verder dan het zetten van een kruisje in het vakje waarmee men instemt met de algemene voorwaarden (de zgn. 'click wrap/accept button'). De betrokkene moet op grond van artikel 7, a) RBP nochtans zijn 'ondubbelzinnige toestemming' verlenen voor de verwerking van persoonsgegevens. Bij het toetreden tot een sociaal netwerk wordt deze toestemming verkregen via het zich akkoord verklaren van de algemene voorwaarden en de privacy statement. Deze lang uitgeschreven en veelal complexe teksten worden slechts zelden geconsulteerd door de gebruikers. Jonge internauten klikken meestal snel door zonder de voorwaarden volledig door te nemen. Men kan zich afvragen of de jonge gebruiker (of zijn/haar ouder of voogd) dan wel werkelijk zijn geïnformeerde en ondubbelzinnige toestemming geeft en of de algemene voorwaarden in dat geval geldig en aanvaardbaar zijn.[154]

63. Wanneer persoonsgegevens van een kind worden verwerkt, is volgens de WG 29 inderdaad de ondubbelzinnige toestemming van zijn of haar wettelijke vertegenwoordiger vereist in de zin van artikel 7, a) van de RBP.[155] De richtlijn bevat echter geen specifieke voorschriften voor de wijze waarop deze toestemming moet worden verkregen noch voor de leeftijdsgrens waaronder de toestemming noodzakelijk is. Deze kwesties worden geregeld in de nationale wetgevingen die verschillen van lidstaat tot lidstaat. Deze leeftijdsgrens is in de meeste lidstaten, maar ook in andere niet-Europese landen, doorgaans gekoppeld aan de leeftijd waarop kinderen geacht worden een bepaalde mate van volwassenheid te hebben bereikt en bekwaam zijn om contractuele verplichtingen te kunnen aangaan.[156] De Belgische WBP voorziet daarentegen geen leeftijdsgrens. Een duidelijkere en geharmoniseerde regeling op Europees niveau is dus wenselijk.

64. Een belangrijke vernieuwing en verbetering naast de invoering van een leeftijdgrens in artikel 8 van de ontwerpverordening is dan ook het verscherpen van de toestemmingsvereiste zelf. Zo wordt in artikel 4, 8) toestemming nu

---

[154] P. VAN EECKE en M. TRUYENS, 'Privacy en sociale netwerken', *supra* noot 8, 123.
[155] WG 29, Advies 2/2009, *supra* noot 24, 9.
[156] De Spaanse wetgeving legt deze grens bijvoorbeeld op 14 jaar. (Zie: Advies van de Europese Toezichthouder voor gegevensbescherming betreffende de mededeling van de Commissie aan het Europees Parlement, de Raad, het Economisch en Sociaal Comité en het Comité van de Regio's – 'Een integrale aanpak van de bescherming van persoonsgegevens in de Europese Unie', *Pb*. C 181/1, 22 juni 2011) In artikel 5 van de Nederlandse WBP ligt deze grens op 16 jaar. (J.M.A. BERKVENS, 'Richtsnoeren publicatie persoonsgegevens op internet', *Computerr.* 2008/132, 199.) De Britse 'Data Protection Act' voorziet geen specifieke leeftijdsgrens, maar de Britse gegevensbeschermingsautoriteit heeft in een aanbeveling deze grens bepaald op de leeftijd van 12 jaar. (http://www.legislation.gov.uk/ukpga/1998/29/contents)

gedefinieerd als 'elke vrije, specifieke, op informatie berustende en *uitdrukkelijke* wilsuiting waarmee de betrokkene, door middel van hetzij een verklaring hetzij een ondubbelzinnige actieve handeling aanvaardt dat hem betreffende persoonsgegevens worden verwerkt'. Voortaan zal dus een expliciete toestemming vereist zijn voor de verwerking en zal een impliciete of stilzwijgende toestemming niet langer aanvaard worden.[157] Overweging 25 verduidelijkt dat de uitdrukkelijke toestemming moet gegeven worden op elke passende wijze die de gebruiker in staat stelt een specifieke en geïnformeerde indicatie te geven omtrent zijn wensen, teneinde te waarborgen dat personen er zich bewust van zijn dat zij toestemming geven. Als voorbeeld wordt gegeven het op een vakje klikken bij een bezoek aan een website. Indien daarenboven de betrokkene zijn toestemming dient te geven na een elektronisch verzoek, moet dat verzoek duidelijk en beknopt zijn. Bovendien wordt in artikel 7 van de ontwerptekst de bewijslast gelegd bij de voor de verwerking verantwoordelijke en heeft de betrokkene het recht zijn toestemming te allen tijde in te trekken.

Ten slotte dient nog opgemerkt te worden dat de ontwerptekst verduidelijkt dat de toestemming uitsluitend gericht is op de verwerking van persoonsgegevens.[158] Dit heeft als gevolg dat wanneer iemand akkoord gaat met de algemene voorwaarden van een SNS, dit niet kan gelijk gesteld worden met een uitdrukkelijke toestemming voor de verwerking van persoonsgegevens. Deze algemene voorwaarden worden immers, zoals boven reeds aangetoond, doorgaans niet of niet volledig gelezen door jonge SNS-gebruikers.[159]

3. Het recht om vergeten te worden

65. Over het zgn. 'right to be forgotten' is sinds enige jaren heel wat discussie geweest op Europees niveau.[160] Een aantal privacygevoelige kwesties hebben het gebrek aan controle aangetoond die de betrokkenen in de praktijk hebben over hun profielgegevens op SNS.[161] De Europese Commissie geeft in een mededeling het voorbeeld aan van een Oostenrijkse rechtenstudent die alle informatie had

---

[157] S. VYNCKE, 'Het voorstel voor een Europese Privacy Verordening doorgelicht', te raadplegen op: http://siriuslegal.wordpress.com/2012/02/06/het-voorstel-voor-een-europese-privacy-verordening-doorgelicht/.

[158] Artikel 6 voorstel algemene verordening gegevensbescherming. Zo wordt ook aangegeven in overweging 25 van de ontwerptekst dat 'de toestemming dient te gelden voor alle verwerkingsactiviteiten die hetzelfde doel of dezelfde doelen dienen'.

[159] Zie: 'Nieuwe Europese privacyregels relevant voor sociale netwerken', 9 maart 2012, http://www.wisemen.nl/weblog/weblogs/nieuwe-europese-privacyregels-relevant-voor-sociale-netwerken/.

[160] J. AUSLOOS, 'The 'Right to be Forgotten' – Worth Remembering?', 30 november 2011, te raadplegen op: http://www.law.kuleuven.be/icri/all_pubs.php?action=pubs_staff&staffid=166&where=. (Hierna J. AUSLOOS, 'Right to be Forgotten') Het recht om vergeten te worden wordt in het Engels ook wel eens 'right to oblivion' genoemd.

[161] J. AUSLOOS, 'Right to be Forgotten', *supra* noot 157, 9-10. Zo is Facebook de afgelopen jaren geregeld in opspraak gekomen wegens schending van de privacy van gebruikers. De 'vind-ik-leuk'-knop werd beschouwd als een schending van de persoonlijke levenssfeer aangezien bij het 'liken' van bepaalde inhoud de persoonlijke gegevens worden doorgestuurd naar de servers van de site in de Verenigde Staten. (Zie: ''Like'-knop van Facebook is illegaal in Europa', HLN 23 augustus 2011, te raadplegen op: http://www.hln.be/hln/nl/4125/Internet/article/detail/1307999/2011/08/23/Like--knop-van-Facebook-is-illegaal-inEuropa.dhtml.)

opgevraagd van op zijn SNS-profiel. De beheerder van de betreffende sociale netwerkdienst zond hem 1224 bladzijden aan informatie door w.o. foto's en berichten van jaren geleden waarvan de student dacht die al lang te hebben verwijderd.[162]

In een mededeling van 2010 definieert de Europese Commissie het recht om vergeten te worden als 'het recht van een persoon om te verkrijgen dat zijn gegevens niet meer worden verwerkt en worden gewist wanneer ze niet langer nodig zijn voor rechtmatige doeleinden'. Samen met het verscherpen van de toestemmingsvereiste moet de introductie van dit recht er voor zorgen dat de betrokkenen daadwerkelijk de zeggenschap behouden over hun eigen persoonsgegevens.[163]

66. In de RBP is geen specifiek 'right to be forgotten' te vinden. Toch zijn er een aantal bepalingen die in die zin geïnterpreteerd kunnen worden.[164] Zo mogen op grond van artikel 6, 1, e) RBP persoonsgegevens niet langer bewaard worden dan noodzakelijk en heeft de betrokkene op grond van artikel 12, b) het recht tot rectificatie, uitwissing of afscherming van de gegevens wanneer de gegevens onvolledig of onjuist zijn. Artikel 14 van de richtlijn voorziet daarenboven een recht tot verzet tegen de verwerking van gegevens (zie randnummer 29).

Om het gebrek aan een duidelijke en afgelijnde bepaling op te vangen, werd een uitgebreid artikel 17 in de ontwerptekst opgenomen. Het eerste lid van het artikel voorziet expliciet het recht om vergeten te worden. De betrokkene moet op elk ogenblik kunnen beslissen om zijn toestemming te herroepen op basis van een aantal gronden en de betreffende persoonsgegevens dienen in dat geval te kunnen worden gewist. In de eerste plaats heeft de betrokkene dit recht indien de gegevens niet langer nodig zijn in verband met de doeleinden waarvoor zij werden verzameld of anderszins werden verwerkt. Tevens geldt dit recht wanneer de overeenkomst die werd gesloten tussen de partijen afgelopen is. Ten slotte kan dit recht worden uitgeoefend wanneer de verwerking van de gegevens in strijd is met de bepalingen uit de verordening.

67. De zinsnede 'met name waar het gaat om persoonsgegevens die door de betrokkene als kind beschikbaar zijn gesteld' in artikel 17 van de ontwerptekst geeft aan dat het recht om vergeten te worden tevens van belang is voor kinderen. Men hoeft hierbij niet enkel te denken aan de situatie van een meerderjarig geworden persoon die bepaalde foto's of andere gegevens uit zijn jeugd wenst te verwijderen. Ook de 16-jarige SNS-gebruiker moet tekst en afbeeldingen van uit zijn of haar vroegere jaren kunnen verwijderen indien de gegevens niet langer noodzakelijk zijn voor bepaalde doeleinden.

---

[162] Europese Commissie, 'Wat betekenen de nieuwe gegevensbeschermingsregels voor sociale netwerken?'. Te raadplegen op: http://ec.europa.eu/justice/data-protection/ document/review2012 /factsheets/3_nl.pdf.

[163] Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's, 'Een integrale aanpak van de bescherming van persoonsgegevens in de Europese Unie, 4.11.2010, COM(2010) 609 definitief, 7 en 8.

[164] J. AUSLOOS, 'Right to be Forgotten', *supra* noot 157,13-14.

68. Artikel 17, 2de lid bepaalt dat in het geval de betrokkene dit recht wens uit te oefenen de voor de verwerking verantwoordelijke alle redelijke maatregelen moet nemen om de gegevens te wissen, tenzij het nodig is de persoonsgegevens te bewaren in de gevallen bepaald in lid 3 van hetzelfde artikel, w.o. het opwegen van het recht op vrijheid van meningsuiting en persvrijheid en het noodzakelijk zijn voor historische, statistische of wetenschappelijke doeleinden. Indien het gegevens betreft die werden doorgegeven door de verantwoordelijke aan derden, dient de verantwoordelijke de derde in te lichten over het verzoek van de betrokkene om iedere koppeling naar, of kopie of reproductie van die gegevens te verwijderen.

69. In de praktijk betekent de nieuwe bepaling dat beheerders van sociale netwerkdiensten, maar ook zoekmachines en andere internetbedrijven, voortaan foto's, video's, berichten of andere UGC op eenvoudig verzoek van de betrokkene zullen moeten verwijderen uit het systeem wanneer er geen gegronde reden is om die gegevens bij te houden. Dat de focus van de nieuwe bepaling sterk ligt op profielgegevens op SNS mag althans duidelijk zijn. De bewijslast wordt bijgevolg gelegd op de schouders van de houders van de persoonsgegevens die op grond van artikel 17 moeten bewijzen dat het voor hen nodig is om de gegevens te bewaren.

4. Het recht om gegevens over te dragen

70. Een andere bepaling van belang voor SNS is artikel 18 dat een recht van gegevensoverdraagbaarheid voorziet. De betrokkene kan op die manier gemakkelijker zijn gegevens van het ene elektronische verwerkingssysteem naar het andere doen overdragen zonder hiervan weerhouden te worden door de voor de verwerking verantwoordelijke. Zo kunnen profielgegevens van het ene sociale netwerk naar het andere worden overgedragen. Bovendien bepaalt artikel 18 dat de betrokkene het recht heeft op een kopie van de gegevens in een elektronisch en gestructureerd formaat.

5. Maatregelen op basis van profilering

71. Artikel 20 bepaalt dat iedere natuurlijke persoon het recht heeft niet onderworpen te worden aan een maatregel waaraan voor hem rechtsgevolgen zijn verbonden of die hem in een aanmerkelijke mate treft en die louter wordt genomen op grond van een geautomatiseerde verwerking die bestemd is om bepaalde aspecten van zijn persoonlijkheid te evalueren of om met name zijn beroepsprestaties, economische situatie, verblijfplaats, gezondheid, persoonlijke voorkeuren, betrouwbaarheid of gedrag te analyseren of te voorspellen. Deze ietwat complex geformuleerde bepaling is een uitwerking van de reeds bestaande regeling voor 'geautomatiseerde besluitsystemen' in artikel 15 RBP. In de ontwerptekst spreekt men nu van 'profilering'. Bij profilering wordt op basis van vooraf vastgestelde criteria uit één of meer gegevensverzamelingen bepaalde

personen geselecteerd, hetzij voor private of commerciële doeleinden, hetzij voor publieke, opsporings- of controletaken.[165]

De gewijzigde bepaling tracht een solide juridische basis te verschaffen ter bescherming van SNS-gebruikers opdat hun privacygevoelige gegevens op hun profiel niet zomaar zouden gebruikt worden voor bepaalde private of publieke maatregelen zonder dat de betrokkene hiervan op de hoogte is. Overweging 58 van de ontwerptekst verduidelijkt dat dergelijke maatregelen alleszins geen betrekking mogen hebben op kinderen.

6. Privacy by default

72. De beginselen 'privacy by design' (ingebouwde privacy) en 'privacy by default' (standaardsysteeminstellingen voor maximale privacy) worden in het nieuwe regelgevend kader erkend als fundamentele beginselen in de gegevensbeschermingsregels.[166] Concreet houdt dit voor de gebruiker in dat hij eigenlijk niet meer zelf de privacy-instellingen hoeft aan te passen, maar dat de sociale netwerkdienst automatisch de meest strikte privacyregels op het profiel moeten toepassen.[167]

[165] Commissie Meijers (Nederland), Verslag betreffende het voorstel voor de herziening van de EU-wetgeving bescherming persoonsgegevens, 2 maart 2012, 3. Te raadplegen op: http://www.eerstekamer.nl/eu/brief2/20120302/notitie_van_de_commissie_meijers/document3. Profilering kan er toe leiden dat de betrokkenen anders worden behandeld of benadeeld worden ten opzichte van andere personen. In het licht van artikel 8 EVRM en artikel 14 EVRM (het discriminatieverbod) is dan ook een strenge regeling uitgewerkt in de ontwerptekst.

[166] Europese Commissie, 'Hoe kan een hervorming de burgers meer bescherming geven', te raadplegen op: http://ec.europa.eu/justice/data-protection/document/review2012/ factsheets /2_nl.pdf.

[167] S. VYNCKE, 'Het voorstel voor een Europese Privacy Verordening doorgelicht', te raadplegen op: http://siriuslegal.wordpress.com/2012/02/06/het-voorstel-voor-een-europese-privacy-verordening-doorgelicht/.

Afdeling 3. Verdiensten en gebreken van het nieuwe voorstel

1. De adviezen van de Europese instanties

73. De WG 29 bracht op 23 maart 2012 een advies uit over het nieuwe voorstel.[168] De werkgroep onderlijnt vooreerst de positieve aspecten van de nieuwe tekst zoals de introductie van een algemeen transparantiebeginsel en de verduidelijking van de toestemmingsvereiste. In het algemeen houdt de ontwerpverordening een versterking in van de rechten van de betrokkenen en is het nieuwe kader consistenter en efficiënter. Toch blijkt de werkgroep in het algemeen niet bijster tevreden te zijn. Zo valt de opname van de regels betreffende politie en justitie in een aparte richtlijn te betreuren aangezien ook op het gebied van handhaving een meer verregaande en diepere harmonisatie noodzakelijk is. De eenmaking van de gegevensbeschermingsregels door middel van een alomvattend gemeenschappelijk kader wordt hierdoor belemmerd.[169]

Ook de Europese Toezichthouder voor Gegevensbescherming (EDPS)[170] benadrukt in zijn advies van 7 maart 2012[171] het gebrek aan harmonisering door de aparte richtlijn. Vele EU-instrumenten betreffende de gegevensbescherming en politionele en gerechtelijke samenwerking blijven op die manier onaangeroerd zodat van een verdere harmonisatie geen sprake is, aldus de EDPS. Wat de materiële bepalingen in de verordening betreft, somt de EDPS de volgende negatieve elementen op: (1) de nieuwe uitzonderingsbepalingen in artikel 21, (2) de mogelijkheid om basisprincipes en -rechten te beperken, (3) de verplichting voor verantwoordelijken voor de verwerking om documenten bij te houden van alle verwerkingsprocessen, (4) de afwijkingen in artikel 44 bij de overdracht van gegevens naar derde landen, (5) de rol van de Europese Commissie bij het uitwerken van nadere regels op grond van artikel 86 en (6) het verplichte

[168] WG 29, Advies 01/2012, *supra* noot 137.

[169] WG 29, Advies 01/2012, *supra* noot 137, 4-5. Zo benadrukt de werkgroep dat 'serious efforts from the European legislator are needed during the legislative procedure to bring the substantive provisions of the Directive closer to those of the Regulation and to ensure consistency in both texts'.

[170] EDPS is de afkorting voor 'European Data Protection Supervisor'. Dit orgaan is een onafhankelijke toezichthoudende autoriteit die erop toeziet dat de Europese instellingen en organen het recht op privacy en de bescherming van persoonsgegevens in acht nemen bij de verwerking van persoonsgegevens en het uitvaardigen van nieuwe beleidslijnen. De Nederlander Peter Hustinx is benoemd als EDPS en de Italiaan Giovanni Buttarelli is adjunct-toezichthouder. (zie: http://nl.wikipedia.org/wiki/Europees Toezichthouder voor gegevensbescherming.) De officiële website is te raadplegen op: http://www.edps.europa. eu/ EDPSWEB/edps/lang/nl/EDPS.

[171] Opinion of the European Data Protection Supervisor on the data protection reform package, 7 maart 2012. Te raadplegen op: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf. Zo stelt de EDPS in punt 441 van zijn verslag: 'the EDPS is, however, seriously disappointed with the proposed Directive for data protection in the law enforcement area. The EDPS regrets that the Commission has chosen to regulate this matter in a self-standing legal instrument which provides for an inadequate level of protection, by far inferior to the proposed Regulation'.

karakter van administratieve sancties.[172] Hierna wordt enkel ingegaan op de voor minderjarigen en SNS gevoelige bepalingen in de ontwerpverordening.

2. Minderjarigen en SNS

2.1 De vrijstelling voor persoonlijke of huishoudelijke doeleinden

74. In artikel 2, § 2, d) van de ontwerptekst is bepaald dat de verordening niet van toepassing is op de verwerking van persoonsgegevens ' door een natuurlijke persoon zonder commercieel belang bij de uitoefening van zijn uitsluitend persoonlijke of huishoudelijke activiteiten'. De zinsnede 'zonder commercieel belang' voegt echter niets belangrijks toe aan de bestaande regeling in artikel 3 RBP (zie randnummer 50) en er wordt spijtig genoeg nog steeds geen inhoudelijke verduidelijking gegeven over deze vrijstelling.[173] Ook de WG 29 vermeldt in haar advies 01/2012 niks over deze uitzondering. Het blijft derhalve onduidelijk in welke gevallen een SNS-gebruiker, die kan kwalificeren als een verantwoordelijke voor de verwerking, zich kan beroepen op de vrijstelling (zie randnummers 50-52).

2.2 Kinderen en minderjarigen

75. De WG 29 is positief over de introductie van artikel 8 in de ontwerptekst op grond waarvan de verwerking van persoonlijke informatie van een kind onder de dertien jaar enkel rechtmatig is indien daarvoor toestemming werd gegeven door de ouder of voogd. De bepaling lijkt een stap in de goede richting te zijn. Toch vindt de werkgroep de bepaling nog te eng aangezien er meer situaties zijn die gereguleerd zouden kunnen worden dan alleen het rechtstreeks aanbieden van diensten van de informatiemaatschappij aan kinderen.[174]

76. De toestemmingsvereiste mag dan wel scherper geregeld zijn, spijtig genoeg werd geen gevolg gegeven aan de *supra* vermelde bezorgdheid over de wijze waarop toestemming voor verwerking van persoonsgegevens moet worden verkregen van het kind via zijn of haar wettelijke vertegenwoordiging (zie randnummers 62-63). Net zoals in de RBP ontbreken enige bepalingen ter zake. Derhalve blijft men aangewezen op de nationale regelgeving. Artikel 8, 3de lid van de ontwerptekst stelt dat de Europese Commissie op grond van artikel 86 gedelegeerde handelingen kan vaststellen om de criteria en vereisten te bepalen ter verkrijging van deze toestemming. De WG 29 heeft zijn twijfels over deze aanvullende taak van de Commissie. Het uitvaardigen van dergelijke maatregelen ter uitvoering van bepaalde artikelen kan immers zeer lang duren en bijgevolg rechtsonzekerheid met zich meebrengen.[175]

---

[172] Zie ook: EDPS Newsletter (N32, maart 2012), 1-3. Te raadplegen op: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Newsletters/Newsletter_32_EN.pdf.

[173] In overweging 15 van de ontwerptekst wordt bovendien hetzelfde voorbeeld gegeven als in overweging 12 van de RBP, nl. het geval van correspondentie of adressenbestanden.

[174] WG 29, Advies 01/2012, *supra* noot 137, 13.

[175] WG 29, Advies 01/2012, *supra* noot 137, 7.

2.3 Het recht om vergeten te worden

77. Ongetwijfeld is de introductie van artikel 17, naast een aantal andere bepalingen zoals het beginsel van 'privacy by default' en het recht tot gegevensoverdraagbaarheid, één van de grote verdiensten van de ontwerpverordening en is deze bepaling in staat de betrokkenen meer controle te geven over de verwerking van hun persoonlijke gegevens.

De Europese wetgever lijkt zich evenwel nog steeds vast te klampen aan de verouderde tweespalt verantwoordelijke/betrokkene van uit de RBP. De tekst gaat volgens de WG 29 voorbij aan de Web 2.0-realiteit van het internet waarin ook derde partijen betrokken zijn die persoonsgegevens gebruiken en verwerken. De verplichting om de persoonsgegevens die door de betrokkene als kind beschikbaar werden gesteld te wissen, geldt in de ontwerptekst enkel voor de verantwoordelijke voor de verwerking. De verantwoordelijke dient op grond van het tweede lid van artikel 17 alle redelijke maatregelen te nemen om derden op de hoogte te stellen dat een betrokkene hun verzoekt iedere koppeling naar, of kopie of reproductie van de persoonsgegevens te wissen. In de online realiteit is het zeer moeilijk voor de verantwoordelijke om alle bestaande kopieën of reproducties te kennen of kan het voorkomen dat na het in kennis stellen van de betrokken derden nieuwe kopieën of reproducties op het net verschijnen.[176] Bovendien verduidelijkt de ontwerptekst niet op welke wijze de betrokkenen het 'right to be forgotten' kunnen uitoefenen indien de verantwoordelijke voor de verwerking niet meer bestaat of niet geïdentificeerd of gecontacteerd kan worden. Derhalve is het aangewezen dat de verplichting om op verzoek van de betrokkene de gegevens te wissen ook wordt ingesteld voor derde partijen opdat de betrokkene zich zou kunnen wenden tot deze derden indien de verantwoordelijke voor de verwerking niet kan gecontacteerd worden.[177]

De gronden in artikel 17, derde lid op grond waarvan de verantwoordelijke onverwijld dient over te gaan tot het wissen van persoonsgegevens zijn ten slotte te beperkt volgens de WG 29. Wanneer links, kopieën of reproducties van persoonlijke informatie niet onder deze gronden vallen, dan is er immers geen mechanisme voorzien om de informatie te laten verwijderen.[178]

2.4 Profilering

78. Volgens de werkgroep is artikel 20 (over de maatregelen op basis van profilering) te wankel geformuleerd om efficiënt toegepast te kunnen worden in een online omgeving.[179] Het zou nader moeten worden aangegeven in de tekst dat ook het creëren van sociale netwerkprofielen onder de toepassing van het artikel valt. Bovendien is de bepaling beperkt tot geautomatiseerde verwerkingen terwijl profilering ook kan voorkomen bij deels geautomatiseerde processen. Op

[176] WG 29, Advies 01/2012, *supra* noot 137, 13.
[177] WG, Advies 01/2012, *supra* noot 137, 14.
[178] WG, Advies 01/2012, *supra* noot 137, 14.
[179] WG, Advies 01/2012, *supra* noot 137, 14. De werkgroep geeft o.a. aan dat de omschrijving 'in aanmerkelijke mate treft' onnauwkeurig geformuleerd is.

die manier wordt onterecht de indruk gewekt dat alle geautomatiseerde beslissingen profileringsbeslissingen zijn.[180]

79. De regeling in het huidige artikel 15 RBP heeft men overigens trachten in overeenstemming te brengen met de Aanbeveling van de Raad van Europa van 23 november 2010 over profilering.[181] In dit beleidsdocument stelt het Comité van Ministers met betrekking tot kinderen het volgende:

'Considering that the profiling of children may have serious consequences for them throughout their life, and given that they are unable, on their own behalf, to give their free, specific and informed consent when personal data are collected for profiling purposes, specific and appropriate measures for the protection of children are necessary to take account of the best interests of the child and the development of their personality in accordance with the United Nations Convention on the Rights of the Child'.

Een loutere verwijzing naar het belang van het kind in overweging 58 van de ontwerpverordening lijkt wat profileringsmaatregelen betreft niet voldoende te zijn om in overeenstemming te zijn met deze aanbeveling van de Raad van Europa.

3. Besluit

80. De poging van de Europese wetgever om de samenhang in het wettelijke kader voor gegevensbescherming te verbeteren en het hoofd te bieden aan de snelle technologische ontwikkelingen in de informatiemaatschappij kan alleen maar worden toegejuicht. Het nieuwe kader tracht het recht op privacy van individuen op het internet te verstevigen door hen een grotere zeggenschap over de eigen gegevens te bieden en tegelijkertijd de verantwoordelijkheid en plichten van de voor de verwerking verantwoordelijke aan te scherpen. Een aantal nieuwe bepalingen in de ontwerpverordening trachten tegemoet te komen aan de nieuwe online Web 2.0.-realiteit van SNS zoals het recht om vergeten te worden, het beginsel van 'privacy default', het recht tot gegevensoverdraagbaarheid en een regeling voor online profilering. Al even vooruitstrevend is het artikel 8 dat rekening houdt met de kwetsbare positie van jonge kinderen op het internet.

81. Toch kan het voorstel niet gespaard worden van kritiek. Vooral over de ontwerprichtlijn waarin de regels voor de voorkoming, onderzoek, opsporing, vervolging en tenuitvoerlegging worden afgezonderd van het harmonisatiepakket kwamen zowel de WG 29 als de EDPS scherp uit de hoek. Belangrijker voor de online privacybescherming van minderjarigen is dat een aantal materiële

[180] DDMA (Dutch Dialogue Marketing Association), 'Reactie op het concept Privacy Verordening', maart 2012, 3. Te raadplegen op: http://ddma.nl/wp-content/uploads/2012/03/DDMA-reactie-concept-EU-Privacy-Verordening-versie-2.pdf.

[181] Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profling, 23 november 2010. Te raadplegen op: https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec(2010)13&Language=lanEnglish&Ver=original&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383.

wijzigingen die rechtstreeks gevolgen met zich meebrengen voor de SNS-sector vaag en inconsistent blijven. Bovendien zijn een aantal problemen die reeds bestonden in de RBP niet opgelost w.o. de betekenis van de vrijstelling voor persoonlijke of huishoudelijke doeleinden in de context van SNS. Zowel rekening houden met de impact van nieuwe Web 2.0.-technologieën op de rechten en plichten van de SNS-gebruikers en -aanbieders en het juiste evenwicht vinden tussen de belangen van alle betrokken actoren blijkt voor de Europese wetgever een moeilijke oefening te zijn.

Vervolgens dringt zich de vraag op naar alternatieve vormen van regulering om niet alleen de bestaande maar ook de toekomstige leemtes in het wetgevende kader op te vullen en meer bewustzijn te creëren bij alle betrokken stakeholders in de SNS-sector.

HOOFDSTUK 3. ALTERNATIEVE REGULERING EN SNS

82. Waar het fundamentele recht op privacy geregeld is in artikel 8 EVRM en de bescherming van persoonsgegevens in de RBP zijn er diverse uitwerkingen te vinden in overeenkomsten, aanbevelingen, gedragscodes en algemene privacy statements.[182] Deze niet-bindende maatregelen zijn vormen van alternatieve regulering. In 2001 vaardigde de Europese Commissie een 'White Paper on European Governance' uit met een aantal principes waarmee in de toekomst rekening dient gehouden te worden bij het uitvaardigen van Europese regelgeving. De Commissie stelde o.a. dat 'wetgeving vaak slechts een onderdeel van een groter geheel vormt waarbij formele regels worden gecombineerd met andere niet-bindende instrumenten zoals aanbevelingen, richtsnoeren of zelfs zelfregulering binnen een gemeenschappelijk afgebakend kader'.[183]

83. Eva Lievens beschreef in haar doctoraat over de bescherming van kinderen en de regulering van media-inhoud de verschillende alternatieve methoden van regulering ('Alternative Regulatory Instruments') die men sinds het begin van het internettijdperk terugvindt in beleidsdocumenten van de Europese instanties.[184] In december 2011 werd door het ICRI een analyse gemaakt van de regelgevende trends met betrekking tot de nieuwe sociale media in het kader van het EMSOC-onderzoeksproject.[185] Voor de bescherming van de privacy van minderjarigen op SNS is het belangrijk even stil te staan bij deze alternatieve vormen van regulering zoals zelfregulering, co-regulering en regulering via technologische maatregelen. Een belangrijke doelstelling van dit onderzoek is immers na te gaan of de bestaande soft law-initiatieven inzake SNS juridisch efficiënt genoeg zijn als alternatief voor of aanvulling op traditionele overheidsregulering.

[182] I. GIESEN, *Alternatieve regelgeving en privaatrecht*, Amsterdam, Kluwer, 2007, 30.
[183] Commissie van de Europese Gemeenschappen, Europese Governance – Een witboek, (COM)2001 428 definitief, 25.07.2001, 23. Te raadplegen op: http://eur-lex.europa.eu/LexUriServ/site/nl/com/2001/com2001_0428nl01.pdf.
[184] E. LIEVENS, *Protecting Children*, *supra* noot 11.
[185] E. LIEVENS e.a., 'State of the art', *supra* noot 34.

Afdeling 1. Van 'command-and-control'-regulering naar alternatieve regulering

1. 'Command-and-control'-regulering

84. Als hoeder van de rechtsstaat dient de overheid de samenleving te ordenen en beschikken de burgers over een set aan fundamentele rechten en plichten waarvan de naleving kan worden afgedwongen voor de rechter. Als men het heeft over overheidsregulering, wetgeving of regelgeving wordt de traditionele vorm van regulering bedoeld waarbij regels door en onder de verantwoordelijkheid van de overheid worden uitgevaardigd en gehandhaafd.[186] De *supra* besproken internationale, Europese en nationale privacyregelgeving valt vanzelfsprekend onder deze categorie. Het volstaat hier te vermelden dat bij zuivere 'command-and-control'-regulering alle regelgevende taken zoals het uitvaardigen, het implementeren, de controle op en de handhaving en afdwinging van de regels enkel voor de overheid zijn weggelegd.[187]

2. Van zelf- naar co-regulering

85. In bepaalde snel evoluerende rechtsgebieden kan zuivere overheidsregulering niet steeds het hoofd bieden aan de complexe aspecten ter zake of een juiste afweging maken tussen de verschillende belangen die betrokken zijn. De gebrekkige bepalingen in de RBP en de nieuwe verordening zijn hier het bewijs van. De gehanteerde regulerende instrumentaria en wetgevingsprocedures zijn vaak ongeschikt om snel en efficiënt een bepaald juridisch en maatschappelijk complex probleem op te lossen.[188] Het mag al duidelijk zijn dat de nieuwe internetomgeving enorme uitdagingen heeft gecreëerd voor beleid en regulering. De onmeetbare snelheid waarmee de technologie vandaag evolueert en de nood aan expertise om complexe sectorale aangelegenheden zoals SNS te reguleren, maakt deze taak van de overheid allesbehalve evident. Het globale karakter van de nieuwe sociale media op het internet heeft de laatste jaren dan ook een verschuiving teweeg gebracht van traditionele naar alternatieve vormen van regulering opdat beleidsmakers sneller en efficiënter zouden kunnen reageren op nieuwe problemen in de internetsector zoals de online privacybescherming op SNS.[189]

86. Aanvankelijk probeerde men het complexe internetgebeuren nog te ordenen door middel van traditionele regulering zoals de Richtlijn Elektronische Handel van 2000 (zie ook randnummer 17).[190] Juist omdat de evoluties van het

---

[186] W.J. WITTEVEEN, I. GIESEN en J.L. DE WIJKERSLOOTH, *Alternatieve regelgeving*, Amsterdam, Kluwer, 2007, 25.
[187] E. LIEVENS, *Protecting Children*, *supra* noot 11, 148.
[188] E. LIEVENS e.a., 'State of the art', *supra* noot 34, 18.
[189] Zie ook: D. VOORHOOF en P. VALCKE (m.m.v. H. CANNIE), *Handboek Mediarecht (3de editie)*, Brussel, Larcier, 2011, 18.
[190] Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt ('richtlijn inzake elektronische handel'), Pb. L 178, 17.7.2000, 1-16.

internet de wetgever steeds achterop hebben doen hinken, werd zelfregulering beschouwd als het ideale instrument om nieuwe elektronische fenomenen op het internet sneller te regelen.[191] Zelfregulering is een begrip met verschillende facetten. Een eenduidige en alomvattende definitie is niet onmiddellijk af te leiden uit de verschillende beleidsdocumenten.[192] Zelfregulering zou men kunnen omschrijven als de wijze van regulering waarbij een groep van private actoren op vrijwillige basis een set van regels creëren, implementeren en afdwingen en waarbij de overheid niet of slecht zeer gering betrokken is. Deze wijze van regulering vindt toepassingen in verschillende sectoren w.o. de mediasector.[193] Voorbeelden ervan zijn gedragscodes, moderators en andere onderlinge sectorale afspraken zoals de 'UK Mobile Operators Code of Conduct' van 2004.[194] Zelfregulering is het grote alternatief voor overheidsregulering of wetgeving opdat het institutionele kader van de overheid in het geheel niet of slechts op een zeer ondergeschikte wijze zou betrokken worden in het besluitvormingsproces.[195] Bij zelfregulering staat de autonomie van de betrokkenen voorop.

87. Na verschillende Europese studies en evaluaties van de zelfreguleringssystemen kwam de idee van een zuivere zelfregulering in een minder goed daglicht te staan. Ondanks de flexibiliteit, het aanpassingsvermogen en de mate van expertise zijn er immers een aantal nadelen aan verbonden: het gebrek aan een effectieve afdwingbaarheid, een laag gehalte van transparantie en toerekenbaarheid en het feit dat private belangen voor publieke belangen kunnen worden geplaatst.[196]

In het 'Action Plan on Better Regulation' van de Europese Commissie waarin één van de maatregelen gericht is op het toenemend gebruik van alternatieve vormen van regelgeving om de beleidsdoelen te bereiken, legt de Commissie meer de nadruk op specifieke vormen van co-regulering. Co-regulering ligt ergens tussen zelfregulering en traditionele regelgeving in. Bij co-regulering wordt getracht de voordelen van de voorspelbaarheid en het bindende karakter van traditionele

---

[191] E. LIEVENS, 'Bescherming minderjarigen online', *supra* noot 5, 62.
[192] E. LIEVENS, 192-193. Voor meer details zie ook: E. LIEVENS e.a., 'State of the art', *supra* noot 34, 27-28.
[193] E. LIEVENS, *Protecting Children*, *supra* noot 11, 190 en 193. Men kan vier types van zelfregulering onderscheiden: (1) pure zelfregulering waarbij de overheid geen sturende of initiërende rol heeft en alle initiatief bij de marktpartijen ligt, (2) associatieve zelfregulering waarbij belangengroepen zelf deelnemen aan de opstelling en uitvoering van regels die het gedrag van groepsgenoten moeten sturen in een richting van een door de groep gewenst doel, (3) wettelijk geconditioneerde zelfregulering waarbij de overheid dwingend bepaalde wettelijke randvoorwaarden vaststelt waarbinnen de marktpartijen zelfregulering kunnen uitvoeren en (4) co-regulering waarbij de overheid en de private sector hun krachten bundelen om tot een beleid te komen. (Zie: A.J.M. VAN BELLEN, *Recht en elektronische handel*, Amsterdam, Kluwer, 2002, 63.)
[194] Voor meer informatie, zie: http://stakeholders.ofcom.org.uk/market-data-research/media-literacy/archive/medlitpub/ukcode/.
[195] W.J. WITTEVEEN, I. GIESEN en J.L. DE WIJKERSLOOTH, *Alternatieve regelgeving*, Amsterdam, Kluwer, 2007, 31. Zelfregulering kan niet onmiddellijk worden begrepen vanuit het publiekrechtelijke beginsel van de scheiding der machten: het gaat veeleer om 'een primaat van het veld of om een opdracht tot verantwoordelijk gedrag aan professionals en andere betrokkenen bij de praktijken die zich in het veld afspelen en door middel van normen gestalte geven aan de afweging van daarin gesitueerde belangen'.
[196] E. LIEVENS, *Protecting Children*, *supra* noot 11, 502.

wetgeving en die van de meer flexibele aanpak via zelfregulering te combineren.[197] Een mooi voorbeeld van co-regulering is het Nederlandse Kijkwijzersysteem (zie ook randnummer 10).[198]

Waar zuivere zelfregulering wordt gekenmerkt door een 'bottom-up'-benadering waarbij de betrokken private sector louter op vrijwillige basis onderlinge afspraken maakt, grijpt de overheid bij co-regulering wel degelijk in. In Europese context spreekt men eerder van een 'top-down'-benadering waarbij de basisvereisten bij wet (lees: verordening, richtlijn of ander EU-instrument) worden vastgesteld en de relevante stakeholders uitgenodigd worden de normen verder uit te werken.[199] De overheid dient hierbij te zorgen voor een juridisch vangnet wanneer het zelfregulerend mechanisme zou tekortschieten. Het verschil tussen zelf- en co-regulering ligt aldus in de mate van overheidsparticipatie.[200]

Voor een gevoelige kwestie zoals de bescherming van online privacy van minderjarigen zou een co-regulerend initiatief wel eens de passende componenten kunnen bevatten teneinde zowel de SNS-aanbieders als de overheid te laten participeren in het besluitvormingsproces en een combinatie na te streven van dwingende basisregels en zelfregulerende principes. De co-regulerende bepalingen moeten evenwel binnen het bestaande wettelijke privacykader blijven en rekening houden met andere fundamentele rechten zoals het recht op vrijheid van meningsuiting (zie ook randnummer 93).

3. Technologische regulering

88. Een derde vorm van alternatieve regulering om de beleidsobstakels in het snel evoluerende digitale tijdperk te overbruggen is het gebruik van technologische maatregelen. [201] Zo werd in de Verenigde Staten en Canada de zgn. 'V-chip' ingevoerd om minderjarigen te beschermen tegen schadelijke inhoud op televisie. De belangrijkste technologische maatregelen in het kader van minderjarigen en het internet zijn filters, leeftijdsverificatiesystemen, controlesystemen voor de ouders e.d.m.[202] Hoewel deze systemen gericht zijn op zgn. 'user empowerment' (zie randnummer 89), stelt zich de vraag in hoeverre ze gebruikt kunnen worden binnen en conform het bredere regelgevende kader van fundamentele rechten.[203]

---

[197] D.M. CURTIN, L.H. PUNT-HEYNING, *Europese integratie*, Amsterdam, Kluwer, 2006, 30.
[198] E. LIEVENS e.a., 'State of the art', *supra* noot 34, 43-45.
[199] D.M. CURTIN, L.H. PUNT-HEYNING, *Europese integratie*, Amsterdam, Kluwer, 2006, 31.
[200] E. LIEVENS, 'Bescherming minderjarigen online', *supra* noot 5, 62 en E. LIEVENS e.a., 'State of the art', *supra* noot 34, 40.
[201] Technologische regulering wordt ook wel eens aangeduid als 'code is law' of 'the answer to the machine is in the machine'. Zie E. LIEVENS, *Protecting Children*, *supra* noot 11, 232; N. VAN EJK, L. ASSCHER, N. BERGER en J. KABEL, *De regulering van media in internationaal perspectief*, Amsterdam University Press, 2005, 14 en C. CLARCK, 'The answer to the machine is in the machine' in P. B. HUGENHOLTZ (ed.), *The Future of Copyright in a Digital Environment*, The Hague: Kluwer Law International, 139.
[202] Zie ook: Verslag Commissie, Bescherming kinderen digitale wereld, *supra* noot 29, 7.
[203] E. LIEVENS, *Protecting Children*, *supra* noot 11, 504 en E. LIEVENS e.a., 'State of the art', *supra* noot 34, 53-54.

Wat de privacybescherming van kinderen op SNS betreft kunnen leeftijdsverificatiesystemen, een vlottere toegang tot de privacystatements (door bijvoorbeeld duidelijke links te plaatsen op het platform) en voorlichtingsapplicaties gericht op jonge gebruikers alvast een stap in de goede richting vormen.

4. 'User empowerment' en mediageletterdheid

89. Omdat betrokkenen tegenwoordig meer en meer controle krijgen over de keuze en de selectie van inhoud en actiever deelnemen bij het genereren en verspreiden van informatie zoals op SNS zijn gebruikers niet meer de louter passieve rechtssubjecten waarvoor de overheid regels uitvaardigt, maar worden zij geacht verantwoordelijke en mediageletterde consumenten te zijn.[204] Via 'user empowerment' tracht men ouders en andere voor kinderen verantwoordelijke personen bewust te maken van de gevaren verbonden aan nieuwe sociale media via allerlei bewustmakingscampagnes en/of technische hulpmiddelen.[205] Zo werd in het kader van het 'ik beslis'-project door uitgeverij Abimo een kinderboek over internet uitgebracht om op een kindvriendelijke manier jonge kinderen te leren hoe zij zich in de digitale mediaomgeving het best gedragen.[206]

De trend van 'user empowerment' loopt parallel met de verschuiving van traditionele naar alternatieve regulering en verlegt (minstens een deel van) de verantwoordelijkheid van de overheid naar bedrijven en consumenten. In de context van minderjarigen en SNS is wat deze visie betreft alvast enige voorzichtigheid geboden. Zoals reeds werd aangegeven zijn SNS-gebruikers (en zeker jonge gebruikers) zich in realiteit veel minder bewust van de gevolgen voor hun privacy bij het plaatsen en verspreiden van persoonlijke informatie en kan men zich de vraag stellen of de gebruiker dan wel werkelijk in staat is zijn rol op te nemen als 'empowered media consumer'. Te veel vertrouwen op de verantwoordelijkheid van gebruikers kan met betrekking tot de bescherming van minderjarigen aldus gevaarlijk zijn.[207]

---

[204] E. LIEVENS e.a., 'State of the art', *supra* noot 34, 49.

[205] E. LIEVENS, 'Bescherming minderjarigen online', *supra* noot 5, 62. Dit uitgangspunt wordt o.a. weerspiegeld in overweging 47 van de Richtlijn Audiovisuele Mediadiensten (Richtlijn 2010/13/EU van 10 maart 2010 betreffende de coördinatie van bepaalde wettelijke en bestuursrechtelijke bepalingen in de lidstaten inzake het aanbieden van audiovisuele mediadiensten ('Richtlijn audiovisuele mediadiensten' of 'AVMD-richtlijn') (gecodificeerde versie).): : 'mediageletterde mensen zijn in staat geïnformeerde keuzes te maken, de aard van de inhoud en de diensten te begrijpen en in hun voordeel te doen met het volledige scala aan mogelijkheden die de nieuwe communicatietechnologieën bieden'. In de reeds vermelde Aanbeveling van het Europees Parlement van 2006 (zie randnummer 13) wordt vastgesteld dat 'ouders, leerkrachten en opleiders meer bewust moeten worden gemaakt van de mogelijkheden van de nieuwe diensten en van de wijzen waarop deze veilig door minderjarigen kunnen worden gebruikt, met name door mediageletterdheid- of media-educatieprogramma's, en bijvoorbeeld door permanente vorming binnen het schoolonderwijs'.

[206] Zie: http://www.privacycommission.be/nl/mediawijs en http://www.ikbeslis.be/.

[207] E. LIEVENS e.a., 'State of the art', *supra* noot 34, 53 en 81.

5. De nieuwe ontwerpverordening

90. In een mededeling van 2010 stelde de Europese Commissie dat niet-wetgevende maatregelen zoals bewustmakingscampagnes in de gedrukte en elektronische media en het verstrekken van duidelijke informatie via websites de betrokkenen en voor de verwerking verantwoordelijken moeten informeren over hun rechten en plichten. Verder bevestigde de Commissie haar oude standpunt dat zelfregulerende initiatieven van de voor de verwerking verantwoordelijken kunnen bijdragen tot een betere handhaving van de gegevensbeschermings-regels. Tot slot wordt ook verwezen naar zgn. EU-certificeringsregelingen zoals bijvoorbeeld 'privacyzegels' die kunnen worden ingevoerd voor processen, technologieën, producten en diensten die aan de privacyregels voldoen.[208]

In de RBP van 1995 werd al een bepaling ingevoerd dat het opstellen van gedragscodes door de sector zelf zou aanmoedigen bij de uitvoering van de richtlijn.[209] In de praktijk is van deze bepaling zeer weinig gebruik gemaakt omdat ze door particulieren als onbevredigend werd ervaren.[210] In een uitgebreider artikel 38 van de ontwerpverordening worden gedragscodes opnieuw aangemoedigd en een nieuw artikel 39 handelt over EU-certificering.[211] Of deze nieuwe bepalingen meer succes zullen hebben, valt nog af te wachten.

6. De Amerikaanse COPPA

91. Ook de Amerikaanse beleidsmakers hadden reeds ten tijde van het uitvaardigen van de COPPA het inzicht verworven dat naast overheidsregulering *sensu stricto* technologische maatregelen, zelfregulering en sensibilisering mogelijke aanvullende pistes zijn om de veiligheid en privacy van kinderen op het internet te verhogen. Zo stelden een aantal softwarefabrikanten die deelnamen aan de voorafgaande besprekingen van de COPPA softwarepakketten ten toon die ontworpen waren opdat ouders toezicht zouden kunnen houden op de online inhoud waaraan kinderen worden blootgesteld. Deze technologie zou volgens de fabrikanten tevens gebruikt kunnen worden om privacygevoelige informatie te controleren en te filteren.[212]

92. Om beheerders van websites aan te sporen bepaalt Sectie 1304 ('Safe Harbors') van de COPPA dat zij kunnen voldoen aan de vereisten van de wet door een aantal 'self-regulatory guidelines' te volgen die opgesteld kunnen worden

---

[208] Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's, Een integrale aanpak van de bescherming van persoonsgegevens in de Europese Unie, 4 november 2010, COM(2010)609 definitief, 9 en 14. Te raadplegen op: http://ec.europa.eu/health/data_collection/docs/com_2010_0609_nl.pdf.
[209] Artikel 27 RBP.
[210] Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's, Een integrale aanpak van de bescherming van persoonsgegevens in de Europese Unie, 4 november 2010, COM(2010) 609 definitief, 14.
[211] In artikel 39 van de ontwerpverordening worden de lidstaten en de Commissie aangemoedigd certificeringsmechanismen voor gegevensbescherming en gegevensbeschermingszegels en –merktekens in te stellen zodat de betrokkenen snel het door de voor de verwerking verantwoordelijken en verwerkers geboden niveau van gegevensbescherming kunnen beoordelen.
[212] Rapport FTC, http://www.ftc.gov/reports/privacy/privacy5.shtm.

door de online bedrijfssector zelf. Dergelijke zelfregulerende initiatieven moeten wel goedgekeurd worden door de FTC en dienen binnen het kader van de wet te blijven. Uit het rapport van de FTC blijkt dat de meerderheid van de industrie voorstander was van zelfregulering. Een aantal leden van de FTC stonden eerder sceptisch tegenover zelfregulerende richtlijnen. Opmerkelijk is dat één commissielid opmerkte dat een adequate online bescherming van kinderen een 'mix of parental participation, consent and control, *as well as some government support* and industry self-regulation' vergt.[213] Ook het concept van co-regulering was de commissie dus niet onbekend.

7. Alternatieve regulering en botsende fundamentele rechten

93. Een belangrijke vereiste voor het slagen van alternatief regulerende initiatieven is dat deze instrumenten binnen het wettelijke kader moeten blijven.[214] Niet alleen dienen zij de wetgeving betreffende de gegevensbescherming te respecteren, maar er moet eveneens rekening worden gehouden met andere fundamentele rechten zoals het recht op vrije meningsuiting in artikel 10 EVRM.[215]

[213] Rapport FTC, http://www.ftc.gov/reports/privacy/privacy5.shtm.

[214] Zo moet alternatieve regulering die bijvoorbeeld gericht is op de bescherming van minderjarigen tegen schadelijke media-inhoud voldoen aan de voorwaarden voldoen van artikel 8, tweede lid EVRM. Ouderlijke controlesystemen, filter- en blokkeringsmechanismen ter bescherming tegen schadelijke inhoud kunnen immers het recht op privacy in het gedrang brengen. (E. LIEVENS, *Protecting Children*, *supra* noot 11, 508-509.)

[215] Hoe steviger men de online privacybescherming wil inbouwen, hoe meer men in het vaarwater kan treden van het fundamentele recht op vrijheid van meningsuiting. Het uitvaardigen van alternatief regulerende instrumenten moet het resultaat zijn van een zorgvuldige afweging tussen het recht op privacy en het recht op vrijheid van meningsuiting. Alternatieve regulering die de privacy van minderjarigen op het internet wil beschermen moet aldus de test van artikel 10, tweede lid EVRM kunnen doorstaan. Het recht op vrije meningsuiting blijft echter buiten het bestek van deze masterproef. Voor een uitgebreide analyse van het recht op vrije meningsuiting op het internet zie: E. LIEVENS, P. VALCKE en D. STEVENS, *Praktijkboek recht en internet. Vrijheid van meningsuiting (Titel II, Hoofdstuk 3)*, Brugge, Vanden Broele, 2005, 77 p. Te raadplegen op: https://www.law.kuleuven.be/icri/publications/730b2_Lievens,Valcke,Stevens_2005_PraktijkboekRechtEnInternet-VrijheidMeningsuiting.pdf?where=.

Afdeling 2. Alternatieve regulering en SNS

94. Het nieuwe internetfenomeen van SNS waarbij niet alleen de gebruiker en de tussenpersoon, maar verschillende belanghebbenden actief zijn, hebben de sector ertoe gebracht om onderlinge afspraken te maken in afwezigheid van of in afwachting van enige concrete en efficiënte regelgeving van overheidswege. Op Europees niveau werden de laatste jaren soft law-initiatieven uitgevaardigd ter bescherming van de privacy op SNS. Zo publiceerde het Europees Agentschap voor netwerk- en informatiebeveiliging (ENISA)[216] in 2007 een 'working paper' met een aantal richtsnoeren voor regelgevende instanties en aanbieders van SNS.[217] Ook internationaal werd aandacht besteed aan het fenomeen van SNS. Op 4 maart 2008 werd door de 'International Working Group on Data Protection in Telecommunications'[218] het Memorandum van Rome aangenomen waarin richtsnoeren werden uitgewerkt voor beleidsmakers, aanbieders en gebruikers van sociale netwerkdiensten betreffende veiligheid en privacy.[219] Andere voorbeelden zijn de 'Joint Statements' die o.a. Facebook en Myspace in 2008 hebben afgesloten met het Amerikaanse Openbare Ministerie waarin een aantal veiligheidsstandaarden werden opgenomen.[220]

95. Het gevestigde wetgevende kader van gegevensbescherming verhindert op geen enkele wijze de uitvaardiging van dergelijke initiatieven. Integendeel wordt in zowel de RBP als de nieuwe ontwerpverordening het opstellen van bijvoorbeeld gedragscodes aangemoedigd. Ook de Amerikaanse beleidsmakers

---

[216] Het ENISA is een agentschap van de EU dat in 2004 werd opgericht en heeft tot taak informatienetwerken en daarmee verstuurde gegevens te helpen beveiligen. (website: http://www.enisa.europa.eu/)

[217] G. HOGBEN (ed.) 'Security Issues and Recommendations for Online Social Networks', ENISA Position Paper No. 1, oktober 2007, te raadplegen op: http://www.enisa.europa.eu/activities/identity-and-trust/past-work-areas/social-networks/security-issues-and recommendations-for-online-social-networks. Het Agentschap wil dat het bewustzijn bij ouders, kinderen en aanbieders wordt gestimuleerd en dat daarvoor campagnes worden georganiseerd. Eveneens beveelt het Agentschap aan om het regelgevend kader te herzien en hierbij meer transparantie op te leggen. Verder wordt ook de inbouw van betere beveiligingssystemen zoals toegangscontrole en filters aangemoedigd. Toch benadrukt het Agentschap eveneens de voordelen van SNS 'not least because they herald the end of passive media, bringing free interactive user-generated content to anyone with an Internet connection'.

[218] Deze internationale werkgroep werd opgericht in 1983 in het kader van de 'International Conference of Data Protection and Privacy Commissioners' op initiatief van de 'Berlin Commissioner for Data Protection' en heeft sindsdien tal van aanbevelingen uitgevaardigd om de bescherming van de privacy in telecommunicatie en sinds de jaren '90 op het internet te verbeteren. (website: http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt)

[219] Memorandum van Rome, goedgekeurd op de 30ste Conferentie van commissarissen voor de bescherming van gegevens en de persoonlijke levenssfeer, Straatsburg, 17 oktober 2008, te raadplegen op: http://www.datenschutz-berlin.de/attachments/461/WP social network services.pdf. Voor beleidsmakers beveelt het Memorandum bijvoorbeeld het volgende aan: de introductie van een recht op anonimiteit op internet of het recht om een pseudoniem te gebruiken, de verplichting om op een eerlijke en duidelijke wijze de persoonsgegevens te verwerken, de verplichting om een meldpunt te voorzien voor inbreuken en uiteraard het in rekening nemen van de privacy. Wat kinderen betreft raadt zij enerzijds de ouders aan om zeer oplettend te zijn bij het gebruik van SNS door hun kinderen en anderzijds de overheden om de aspecten van privacy op deze sites te integreren in het onderwijscurriculum.

[220] Voor Facebook zie: Joint Statement on Key Principles of Social Networking Sites, 8 mei 2008. Te raadplegen op: http://www.state.tn.us/attorneygeneral/cases/facebook/facebookstatement.pdf.

opteerden voor een bepaling in de COPPA die de nodige ruimte moest laten voor zelfregulering (zie randnummers 91-92). In het licht van de vluchtige technologische evolutie op het internet kan zelfregulering immers een snelle oplossing zijn omwille van de inherente flexibiliteit, het aanpassingsvermogen en de expertise van de SNS-sector.

Onder deze afdeling wordt de nodige aandacht besteed aan twee recente Europese initiatieven: nl. de 'Safer Social Networking Principles for the EU' (EU-SSNP) van 2009 en de Aanbeveling van de Raad van Europa van 4 april 2012.

1. De 'Safer Social Networking Principles for the EU'[221]

96. Als onderdeel van de 'Digitale Agenda voor Europa'[222] en in het verlengde van het reeds vermelde actieplan van de EU werd vanaf 2008 aandacht besteed aan het fenomeen van de SNS. Tussen de Europese Commissie en de grootste sociale netwerken werd in 2009 een samenwerkingsovereenkomst gesloten over de beveiliging van SNS: de zgn. 'Safer Social Networking Principles for the EU' (EU-SSNP). De SNS-aanbieders hebben in overleg met de Commissie een aantal principes uitgewerkt in dit zelfregulerend instrument die in acht dienen genomen te worden om de veiligheid van kinderen en jongeren op SNS aan te scherpen. Een van de kernelementen van de principes is dat zij een samenwerking beogen tussen alle relevante belanghebbenden w.o. de SNS-aanbieders, ouders, leerkrachten, overheidsinstellingen, politie, justitie, de civiele maatschappij en de gebruiker zelf.[223] De principes zijn in feite niet nieuw of revolutionair, maar zijn gebaseerd op reeds bestaande visies in alternatief regulerende beleidsdocumenten die de laatste jaren werden uitgevaardigd. Tot op heden hebben eenentwintig ondernemingen de beginselen ondertekend waaronder Facebook, Google, MySpace en Netlog.[224]

97. Hieronder worden de zeven overeengekomen principes toegelicht. De contracterende sociale netwerkdiensten dienen de principes te implementeren en ondersteunen. Door middel van een 'self-declaration'-formulier dient de Europese Commissie op de hoogte te worden gehouden zodat de Commissie de efficiëntie en handhaving van de overeenkomst op termijn kan evalueren (zie randnummers 98-101).

---

[221] Zie: 'Safer Social Networking Principles for the EU', 10 februari 2009, te raadplegen op: http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf. (Hierna: EU-SSNP 2009)

[222] De digitale agenda van de Europese Commissie is één van de zeven pijlers van de strategie Europa 2020 die bepaalde groeidoelstellingen voor de Europese Unie tegen 2020 vooropstelt. Deze digitale agenda stelt voor om het potentieel van de informatie- en communicatietechnologieën beter te benutten om innovatie, economische groei en vooruitgang te stimuleren (http://europa.eu/legislation_summaries/information_society/strategies/si0016_nl.htm). De officiële website is te raadplegen op: http://ec.europa.eu/information_society/digital-agenda/index_en.htm.

[223] E. LIEVENS e.a., 'State of the art', *supra* noot 34, 59.

[224] Digitale agenda: 'sociale netwerken kunnen meer doen om de privacy van minderjarigen te beschermen', 30 september 2011. Persbericht te raadplegen op: http://www.europa-nu.nl/id/vit6g2bgsjwz/nieuws/ digitale_agenda_sociale_netwerken_kunnen?ctx=vidymbu7mlv1.

1.1 De zeven principes

1) MAAK GEBRUIKERS, OUDERS/VERZORGERS EN LEERKRACHTEN OP EEN OPVALLENDE, DUIDELIJKE EN VOOR DE BETREFFENDE LEEFTIJD GESCHIKTE MANIER BEWUST VAN EDUCATIEVE BOODSCHAPPEN OVER VEILIGHEID EN OVER DE GEBRUIKSVOORWAARDEN

Ouders en leerkrachten spelen een cruciale rol in de online veiligheid van kinderen. Aanbieders van sociale netwerkdiensten zouden hen dan ook voldoende en duidelijk moeten inlichten opdat zij op hun beurt kinderen kunnen informeren over hun veiligheid en privacy.

2) ZORG ERVOOR DAT DE DIENSTEN GESCHIKT ZIJN VOOR DE LEEFTIJD VAN DE DOELGROEP.

SNS-aanbieders zouden hun systeem kindvriendelijk moeten maken en beheren opdat de kans op ongeschikte inhoud en ongewenst contact zo laag mogelijk blijft. Dergelijke maatregelen kunnen bijvoorbeeld zijn: duidelijk weergeven wanneer bepaalde diensten niet geschikt zijn voor kinderen of wanneer een minimumleeftijd van toepassing is, de nodige stappen ondernemen om minderjarigen te identificeren en te verwijderen van hun diensten, vermijden a.d.h.v. bepaalde maatregelen zoals cookies die gebruikers trachten te herregisteren d.m.v. een bepaalde (meerderjarige) leeftijd, ouderlijke toezichtsystemen aanmoedigen, de mogelijkheid en middelen voorzien om technische maatregelen zoals labelling, rating en leeftijdsrestricties te gebruiken enz.

3) GEEF GEBRUIKERS CONTROLE DANKZIJ HULPMIDDELEN EN TECHNOLOGIE

Aanbieders zouden moeten de nodige tools en technologie ter beschikking stellen om kinderen en minderjarigen te helpen bij het raadplegen van informatie en hierbij zelf controle te hebben over welke inhoud als geschikt wordt beschouwd ('user empowerment'[225] (zie randnummer 89)). Zo dient men ervoor te zorgen dat private profielen van minderjarigen niet kunnen worden opgezocht via externe zoektrobots, dat profielen van minderjarigen automatisch op 'privé' kunnen worden gezet en moet de mogelijkheid worden geboden om een bepaalde gebruiker te blokkeren of te weigeren op bepaalde verzoeken.

4) STEL GEBRUIKSVRIENDELIJKE PROCEDURES TER BESCHIKKING OM GEDRAG OF INHOUD DIE IN STRIJD IS MET DE ALGEMENE VOORWAARDEN TE MELDEN

Dergelijke procedures zouden gemakkelijk toegankelijk, eenvoudig en leeftijdsgeschikt dienen te zijn. Aanbieders van sociale netwerkdiensten geven dergelijke proceduremechanismen best aan in de gebruiksvoorwaarden. Bovendien moeten beheerders snel kunnen reageren op klachten.

5) ANTWOORD OP MELDINGEN VAN ILLEGALE INHOUD OF GEDRAG

[225] Zie ook E. LIEVENS, *Protecting Children*, *supra* noot, 237.

Aanbieders zouden moeten beschikken over efficiënte mechanismen om potentieel illegale inhoud te beoordelen en te verwijderen. Bovendien moeten zij klachten kunnen doorgeven aan politie en justitie via hotlines.

6) STEL DE GEBRUIKERS IN STAAT EN MOEDIG HEN AAN OM VEILIG OM TE GAAN MET PERSOONSGEGEVENS EN PRIVACY

Aanbieders zouden standaard privacy-instellingen met bijbehorende informatie ter beschikking moeten stellen om gebruikers aan te moedigen om een geïnformeerde beslissing te nemen over welke informatie ze online willen beschikbaar stellen. Gebruikers moeten gewaarschuwd worden wanneer bepaalde handelingen implicaties kunnen inhouden voor hun privacy. Gebruikers moeten in staat zijn om hun privacy-status of-instellingen op elk moment te raadplegen. Zeker voor kinderen en jongeren is dit principe uitermate belangrijk voor de bescherming van hun privacy.

7) EVALUEER DE MIDDELEN VOOR HET BEOORDELEN VAN ILLEGALE OF VERBODEN INHOUD/GEDRAG

Gedurende het verloop van het beheer van de SNS zouden aanbieders hun eigen systeem periodiek moeten evalueren en verslag uitbrengen bij de Europese Commissie opdat potentiële risico's voor minderjarigen op tijd kunnen worden geïdentificeerd en verholpen.

1.2 Evaluatie door de Europese Commissie: 'yet much remains to be done'[226]

98. De Europese Commissie publiceerde zijn eerste evaluatierapport op 9 februari 2010. Door een team van onderzoekers werden na een analyse van de ingediende evaluatieformulieren 25 profielsites getest aan de hand van vragenlijsten.[227] De resultaten uit het rapport waren niet zo bevredigend. Minder dan de helft van de aangesloten SNS slaagde erin profielen van minderjarigen enkel zichtbaar te maken voor vrienden. Slechts de helft van de sites nam de vereiste maatregelen opdat online profielen van minderjarigen niet via een zoekrobot zouden kunnen worden opgezocht. Bovendien waren er maar negen sites die werkelijk antwoordden op privacygerelateerde vragen gesteld door minderjarigen.[228]

---

[226] V. REDING, 'Think before you post! How to make social networking sites safer for children and teenagers?', Speech op de Safer Internet Day, Straatsburg, 9 februari 2010. Te raadplegen op: http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/22&format=HTML&aged=0&language=EN&guiLanguage=en.

[227] De volgende SNS werden getest: Arto, Bebo, Dailymotion, Facebook, Giovani.it, Youtube (Google), Hyves, Xbox Live (Microsoft), Windows Live (Microsoft), MySpace, Naszaklaza.pl, Netlog, One.lt, Piczo, Ratee, Skyrock, SchulerVZ (VZnet), StudiVZ (VZnet), meinVZ (VZnet), Habbo Hotel (Sulake), IRC Galleria (Sulake), Tuenti, Yahoo! Answers, Yahoo! Flickr en Zap.lu.

[228] Het rapport van de Commissie en de evaluatieformulieren van de SNS-beheerders zijn te raadplegen op: http://ec.europa.eu/information_society/activities/_social_networking/eu_action/implementation_princip_2010/index_en.htm.

99. Als we even het voorbeeld aanhalen van de Belgische SNS Netlog[229] blijkt dat verdere inspanningen noodzakelijk zijn om de gebruikers over hun rechten en plichten te informeren en de bescherming van de privacy ten volle te garanderen. Hoewel Netlog verschillende privacy-instellingen voorziet en eenvoudige toegang verschaft tot de algemene voorwaarden en het privacybeleid, wordt er weinig informatie gegeven over het gebruik ervan en de mogelijke gevolgen van het bekendmaken van bepaalde informatie. Gebruikers worden wel gewezen op de gevaren voor hun veiligheid op de site, maar er wordt geen informatie verschaft voor ouders en leerkrachten. Niettemin is Netlog nog één van de betere leerlingen van de klas en voorziet een meldknop voor misbruik. Opvallend is ook dat men op Netlog net zoals op Facebook onder de dertien jaar niet kan registeren. Nochtans weerhoudt deze laatste maatregel jonge kinderen er niet van om onder een valse leeftijd een profiel aan te maken.

100. In juni en september 2010 werden de SNS nogmaals geëvalueerd. Hoewel de meeste SNS specifiek op minderjarigen afgestemde informatie over veiligheid en algemene voorwaarden ter beschikking stelden, waren de resultaten wederom teleurstellend. Slechts twee SNS stelden standaardinstellingen in die het persoonlijk profiel van minderjarigen alleen openstellen voor een lijst van goedgekeurde contactpersonen. Op tien door de Europese Commissie geteste sites waren profielen van minderjarigen nog steeds rechtsreeks toegankelijk voor vrienden van vrienden. Toch maakten nu twaalf SNS het onmogelijk om profielen van minderjarigen te vinden via zoekrobots. [230]

101. De resultaten van de onderzoeksrapporten tonen de zwaktes aan van het zelfregulerend karakter van de overeenkomst. De principes zijn niet juridisch afdwingbaar, maar dienen enkel als richtsnoeren waarbij elke aanbieder van een SNS zelf de reikwijdte en de wijze van implementatie bepaalt ter uitvoering van deze beginselen.[231] Het gebrek aan een afdwingingsmechanisme ontmoedigt de naleving door de aangesloten SNS en verhindert de totstandkoming van een geharmoniseerd pakket van verplichtingen ter bescherming van de privacy van jonge SNS-gebruikers.[232]

2. Aanbeveling van de Raad van Europa van 4 april 2012

102. De Raad van Europa is zich tevens bewust van de implicaties van SNS op het fundamentele recht op privacy. Een interessant beleidsdocument hieromtrent

---

[229] Netlog werd getest en geëvalueerd door Prof. Dr. Michel Walrave van de Universiteit van Antwerpen (MIOS). Het verslag is te raadplegen op: http://ec.europa.eu/information_society/activities/social_networking/docs/translated_reports_10/netlog.pdf.

[230] Europese Commissie (persbericht), 'Digitale Agenda: sociale netwerken kunnen meer doen om de privacy van minderjarigen te beschermen', 30 september 2011, te raadplegen op: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/1124&format=HTML&aged=0&language=NL&guiLanguage=en en Europese Commissie (persbericht), 'Digitale Agenda: slechts twee socialenetwerksites bieden automatisch privacybescherming voor profiel van minderjarigen', 21 juni 2011, te raadplegen op: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/762&format=HTML&aged=1&language=NL&guiLanguage=en.

[231] 'These principles are aspirational and not prescriptive or legally binding, but are offered to service providers with a strong recommendation for their use.' (EU-SSNP 2009, *supra* noot 218, 1.)

[232] E. LIEVENS e.a., 'State of the art', *supra* noot 34, 61.

is de recente Aanbeveling van het Comité van Ministers betreffende de bescherming van mensenrechten met betrekking tot sociale netwerkdiensten.[233] Op te merken valt dat ook dit instrument niet bindend is, maar niettemin een belangrijke morele waarde bekleedt.

103. In de Aanbeveling worden ten eerste de voordelen van SNS voor de fundamentele mensenrechten onderlijnd w.o. de stimulering voor de vrijheid van meningsuiting en vrijheid van informatie. Daarna worden de gevaren aangegeven die SNS kunnen doen ontstaan voor het recht op vrijheid van meningsuiting en informatie en het recht op eerbiediging van het privéleven, nl. de onvoldoende bescherming van kinderen en jongeren tegen schadelijke inhoud of gedrag, miskenning van rechten van anderen, het gebrek aan 'privacy friendly default'-instellingen en het gebrek aan transparantie wat betreft het doel waarvoor persoonlijke informatie wordt verzameld en verwerkt.[234]

Om tegemoet te komen aan deze bedreigingen worden reeds bekend in de oren klinkende aanbevelingen gericht naar de verdragsstaten zoals het verhogen van het bewustzijn en de mediageletterdheid bij gebruikers, het verbeteren van de transparantie bij de verwerking van persoonsgegevens en het uitbouwen van zelf- en co-regulerende mechanismen waar dit aangewezen is. Tevens worden lidstaten aangemaand om informatie en maatregelen te voorzien om gebruikers van sociale netwerkdiensten te helpen bij het begrijpen van de instellingen op hun profiel, de controle van hun informatie en om geïnformeerde keuzes te maken.[235]

104. In een appendix worden de voorgestelde maatregelen opgesplitst in drie actiedomeinen. Het eerste betreft de informatie die gebruikers delen op sociale media. Zo moeten volgens de Raad gebruikers erop kunnen vertrouwen dat de informatie die ze vrijgeven op een gepaste manier wordt verwerkt. Tevens moeten gebruikers zich bewust zijn van de gevolgen wanneer ze bepaalde informatie op een SNS plaatsen. Gebruikers moeten hierover worden geïnformeerd. Specifiek voor minderjarigen wijst de Raad op de bewustmaking van ouders, voogden en leerkrachten om jongere kinderen te begeleiden bij het beheren van hun online profiel.[236]

In een tweede actiedomein besteedt de Raad uitgebreid de aandacht aan de bescherming van kinderen en jongeren tegen schadelijke inhoud en gedrag op SNS. De Raad benadrukt dat SNS een steeds belangrijkere rol spelen in het leven van kinderen en jongeren, op het gebied van hun persoonlijke ontwikkeling en op het gebied van hun deelname aan het sociale leven. Omwille van de kwetsbaarheid van kinderen en jongeren verdienen zij extra bescherming en ligt de verantwoordelijkheid hiervoor zowel bij de ouders of voogden, leerkrachten als bij de SNS-

[233] Recommendation CM/Rec(2012)4 of the Committee of Ministers to member States on the protection of human rights with regard to social networking services, 4 april 2012. Te raadplegen op: https://wcd.coe.int/ViewDoc.jsp?id=1929453&Site=CM. (Hierna: Aanbeveling RvE SNS)
[234] Aanbeveling RvE SNS, *supra* noot 230, overwegingen 1-2.
[235] Aanbeveling RvE SNS, *supra* noot 230, overwegingen 3-4.
[236] E. WAUTERS, 'Mensenrechten en sociale media', 18 april 2012, http://emsoc.be/3298-mensenrechten-en-sociale-media/.

beheerders. [237] De Raad stelt de volgende maatregelen voor die wederom niet nieuw in de oren klinken en gebaseerd zijn op reeds bestaande beleidsvisies, maar vooral in verhouding met de fundamentele bepalingen uit het EVRM (w.o. artikelen 8 en 10) worden geplaatst:

'In co-operation with the private sector and civil society, member States should take appropriate measures to ensure children and young people's safety and protect their dignity while also guaranteeing procedural safeguards and the right to freedom of expression and access to information, in particular by engaging with social networking providers to carry out the following actions:

– provide clear information about the kinds of content or content-sharing or conduct that may be contrary to applicable legal provisions;

– develop editorial policies so that relevant content or behaviour can be defined as 'inappropriate' in the terms and conditions of use of the social networking service, while ensuring that this approach does not restrict the right to freedom of expression and information in the terms guaranteed by the European Convention on Human Rights;

– set up easily accessible mechanisms for reporting inappropriate or apparently illegal content or behaviour posted on social networks;

– share best practices on ways to prevent cyber-bullying and cyber-grooming. In this connection, age-differentiated access should be treated carefully where age is provided by children and young people themselves. Social networking providers should take diligent action in response to complaints of cyber-bullying and cyber-grooming.

In addition, member States should:

– encourage the establishment of transparent co-operation mechanisms for law-enforcement authorities and social networking services. This should include respect for the procedural safeguards required under Article 8, Article 10 and Article 11 of the European Convention on Human Rights;

– ensure respect for Article 10, paragraph 2, of the European Convention on Human Rights. This includes refraining from the general blocking and filtering of offensive or harmful content in a way that would hamper its access by users. In this connection, the Committee of Ministers' Recommendation CM/Rec(2008)6 on measures to promote the respect for freedom of expression and information with regard to Internet filters should be implemented with a view to ensuring that any decision to block or delete content is taken in accordance with such principles. Transparent voluntary individual filtering mechanisms are also to be encouraged.'[238]

Ten slotte wordt in een laatste actiedomein de problematiek van de verwerking van persoonlijke gegevens behandeld waarbij de Raad een verhoogde bescher-

[237] Aanbeveling RvE SNS, *supra* noot 230, overwegingen 6-7.
[238] Aanbeveling RvE SNS, *supra* noot 230, overwegingen 10-11.

ming van gevoelige gegevens, betere veiligheidsmaatregelen en meer transparantie aangeeft als richtlijnen.[239]

3. Besluit

105. Al enige jaren zijn er zelfregulerende instrumenten beschikbaar met richtsnoeren voor SNS-gebruikers, -aanbieders en de overheid. Uit de twee instrumenten die werden besproken blijkt dat de aanbevelingen inhoudelijk vooral gericht zijn op het aanmoedigen van SNS-aanbieders om duidelijke en leeftijdsgeschikte algemene voorwaarden en privacy statements te voorzien. Bovendien zouden aanbieders duidelijke informatie moeten ter beschikking stellen over de veiligheidsrisico's op de SNS. Door middel van gebruiksvriendelijke een aangepaste 'privacy default'-instellingen moet de gebruiker meer controle krijgen over de online uitstorting van zijn persoonlijke gegevens. Indien aanbieders op een heldere wijze de rechten en plichten uiteenzetten waarnaar een duidelijke link is aangegeven, zullen gebruikers en hopelijk ook de minderjarige gebruikers misschien de moeite doen om daadwerkelijke kennis te nemen van de algemene voorwaarden.[240] De Aanbeveling van de Raad van Europa is hoofdzakelijk gericht naar de verdragsstaten die een positieve plicht hebben om gepaste maatregelen te nemen en beleidslijnen uit te stippelen teneinde kinderen te behoeden voor een schending van hun privacy op SNS. Tevens wordt de rol van de ouders en leerkrachten benadrukt die bewuster moeten worden gemaakt van de risico's teneinde kinderen weerbaarder te maken tegen miskenning van hun persoonlijke levenssfeer.

106. De werkelijke impact van de aanbeveling van de Raad van Europa valt nog af te wachten, maar de periodieke evaluaties van de Europese Commissie na het aannemen van de EU-SSNP demonstreren alvast de beperkingen van het zelfregulerend karakter van de initiatieven. Vooreerst is de afwezigheid van enig efficiënt afdwingbaarheidsmechanisme één van de grote zwaktes van de twee instrumenten. Bovendien zou de SNS-sector geneigd kunnen zijn naast privacy-voorschriften en -instellingen voor de gebruikers onderlinge kartelafspraken te maken zodat zich een miskenning van de mededingingsregels kan voordoen. Private belangen zouden op die manier vóór openbare belangen worden geplaatst en samen met het gebrek aan afdwingbare bepalingen leiden tot een 'democratisch deficit'.[241]

Op een gestage wijze is toch enige vooruitgang merkbaar in het privacybeleid van de betrokken SNS en op termijn zou dit nog moeten kunnen verbeteren. Nochtans zouden doelmatige handhavingsbepalingen de naleving kunnen opdrijven. Bovendien zouden dergelijke zelfreguleringsinitiatieven gelinkt kunnen worden aan de bestaande wettelijke voorschriften om enerzijds de SNS-sector te doen participeren in het besluitvormingsproces en anderzijds te kunnen terugvallen op voldoende evenwichtige kernbepalingen bij de vaststelling van een inbreuk.

---

[239] Aanbeveling RvE SNS, *supra* noot 230, overwegingen 12-15.
[240] Zie ook: R. VAN DEN HOVEN VAN GENDEREN, 'Algemene voorwaarden', *supra* noot 41, 106.
[241] Zie ook E. LIEVENS, *Protecting Children*, *supra* noot 11, 205-206.

107. Om de privacy van jonge SNS-gebruikers op de meest doeltreffende manier te beschermen lijkt co-regulering de betere uitweg te zijn. Co-regulering wordt in de rechtsleer beschouwd als een meer verfijnd instrument dan zelfregulering omdat het een combinatie inhoudt van de voordelen van zowel zelfregulering als traditionele overheidsregulering ('the best of both worlds').[242] Binnen het kader van de bestaande fundamentele privacybepalingen (artikel 8 EVRM en artikel 16 VN-Kinderrechten-verdrag) en de nieuwe regels voor de online gegevensbescherming in de ontwerpverordening zouden nieuwe initiatieven kunnen worden uitgewerkt die inhoudelijk de principes bevatten van de bestaande zelfreguleringsinstrumenten zoals de EU-SSNP en de Aanbeveling van de Raad van Europa, maar tegelijkertijd voorzien in dwingende bepalingen. Nochtans is de nodige voorzichtigheid geboden bij de structurering en de uitwerking van een co-regulerend kader. Alle participerende actoren moeten in rekening worden genomen en bij het opstellen van voorschriften moeten andere fundamentele mensenrechten w.o. het recht op vrijheid van meningsuiting gerespecteerd worden.

[242] E. LIEVENS, *Protecting Children*, *supra* noot 11, 503.

HOOFDSTUK 4. CONCLUDERENDE BESCHOUWINGEN

1. Vormt de nieuwe ontwerpverordening een oplossing voor de privacyrisico's voor minderjarigen op SNS?

108. De elektronische omgeving waarin gebruikers en aanbieders op een vrij onvoorzichtige wijze omgaan met persoonsgegevens zal blijven evolueren. Op die manier evolueert ook de houding van gebruikers, aanbieders en regelgevende instanties tegenover privacy. De oubollige uitgangspunten in de huidige gegevensbeschermingsregels zijn moeilijk te transponeren op de verhouding tussen aanbieders, gebruikers en derden op SNS. De open interpretatie van de toestemmingsvereiste bij het registreren op een SNS maken de weg vrij voor aanbieders om de waarborgen die de huidige regels bieden uit te hollen en de persoonsgegevens voor allerhande commerciële doeleinden te gebruiken.[243] De verschillende belanghebbenden die betrokken zijn in het complexe spectrum van SNS maken de toepassing van de bestaande regels bijzonder moeilijk.

Het nieuwe voorstel tot verordening is daarom welgekomen en wil de moderne online privacyproblematiek op SNS verhelpen door zowel gebruikers als aanbieders stevigere wettelijke garanties te bieden die meer up-to-date zijn dan de bepalingen van de RBP. Nieuwe bepalingen zoals het recht om vergeten te worden en het beginsel van 'privacy by default' kunnen worden toegejuicht. Na een tijdperk van zelfregulering en sensibilisering opteert de Europese wetgever er voor de problematiek van online privacy van kinderen onder de dertien jaar te incorporeren in het algemene kader betreffende gegevensbescherming. Een aantal problemen onder de huidige richtlijn worden daarenboven aangepakt en oude concepten worden in een nieuw jasje gestoken.

Niettemin benadrukken de Europese gegevensbeschermingsinstanties in hun adviezen dat een aantal van de nieuwe bepalingen meer uitwerking behoeven en dat de doelstelling van een alomvattend en geharmoniseerd wettelijk privacykader in het water is gevallen door de handhaving door de lidstaten afhankelijk te maken van een aparte richtlijn.

2. Wat is dan de beste regelgevende strategie?

109. De overheid kan niet op zijn eentje de impact van de verschillende beleidsopties op de online privacybescherming van minderjarigen correct inschatten. Zonder de nodige kennis en expertise van de SNS-sector zal het resultaat van loutere 'command-and-control'-regulering, al dan niet binnen het kader van de gegevensbescherming, niet bevredigend zijn. Daarenboven is er het risico dat tijdens het besluitvormingsproces de online omgeving reeds verder geëvolueerd zal zijn. Is dit niet het geval, dan zal dit onvermijdelijk gebeuren na de totstandkoming van de wetgeving. De huidige Web 2.0.-toepassingen zijn nu

[243] Zie ook P. VAN EECKE en M. TRUYENS, 'Privacy en sociale netwerken', *supra* noot 8, 127-128.

al aan het afstevenen op een integraal semantisch netwerk (Web 3.0.) waarbij verschillende online diensten met elkaar zijn verbonden en de controle op de gegevensstroom nog complexer zal worden. De nieuwe bepalingen in de ontwerpverordening die afgestemd zijn op SNS zullen op hun beurt komen te verouderen. Het lijkt mij daarom aannemelijk te stellen dat voor minderjarigen en SNS de nieuwe ontwerptekst wel een vooruitgang betekent en een stap in de goede richting lijkt te zijn, maar op termijn hoogstwaarschijnlijk niet tot de verhoopte resultaten zal leiden en hetzelfde lot zal ondergaan als de huidige richtlijn. Indien aangepaste gegevensbeschermingsregels zich dan wederom jarenlang op zich laten wachten blijft de wetgever dweilen met de kraan open.

110. Het opstellen van regels volledig laten afhangen van de SNS-sector zelf is dan ook weer niet aangewezen. Privacy wordt niet meteen hoog in het vaandel gedragen door de SNS-aanbieders zelf en private belangen zouden voor openbare belangen worden geplaatst. De overheid dient hoe dan ook betrokken te worden in het besluitvormingsproces en moet een algemeen kader verschaffen dat de nodige waarborgen biedt op basis waarvan de SNS-sector nadere privacyregels kan implementeren. Alle relevante actoren moeten hierbij geraadpleegd worden en bewust gemaakt worden van de potentiële privacyrisico's voor minderjarigen. De nieuwe ontwerpverordening mag dan wel in enig opzicht zorgen voor een meer transparante gegevensverwerking en modernere principes die aangepast zijn aan de SNS-realiteit en de kwetsbare positie van kinderen onder de dertien jaar, het zijn tenslotte de betrokken spelers die de drijvende kracht moeten vormen voor een verbetering en modernisering van het regulerend kader.

111. Met de komst van de nieuwe verordening lijkt het er op dat de alternatieve instrumenten m.b.t. SNS veeleer fungeren als een tussentijdse oplossing en een soort van reddingsmiddel zijn in afwachting van specifiek op sociale media en minderjarigen geschoeide hard law-bepalingen. De naleving ervan door SNS-aanbieders blijft immers beperkt. Toch vallen bepaalde aspecten zoals het instellen van technische beveiligingssystemen niet gemakkelijk te transformeren naar een afdoende dwingende wettekst en is de hulp van de SNS-sector een onmisbare vereiste bij het uitvaardigen van meer technische privacyvoorschriften om het wettelijke basiskader aan te vullen. Nu co-regulering de meest aangewezen regelgevende strategie lijkt te zijn, stelt zich de vraag hoe het wettelijk kader (naast de huidige Europese visie van integratie van online privacyaspecten in het gegevensbeschermingskader) op basis waarvan de sector aanvullende voorschriften zou moeten opstellen er dan zou kunnen uitzien.

3. Wat zijn de reguleringsopties?

112. Vooreerst zou men zoals de Amerikaanse wetgever een specifiek wettelijk instrument op EU-niveau in het leven kunnen roepen dat uitsluitend gericht is op de online privacybescherming van kinderen. Het toepassingsgebied zou i.t.t. de Amerikaanse COPPA echter eveneens de minderjarigen die ouder zijn dan dertien jaar moeten bestrijken. Jongeren zijn vaak actiever op SNS dan jonge kinderen en hebben in dit opzicht minstens evenveel recht op een adequate bescherming

van hun privacy. De incorporatie van de geschikte leeftijdsdrempels zou men kunnen houden voor de zelfregulerende aanvullingen op de wettelijke regels waarin bijvoorbeeld strengere voorwaarden gelden voor kinderen onder de dertien jaar (w.o. bijvoorbeeld een werkelijke onmogelijkheid om te registeren op een SNS zodat jonge kinderen de leeftijdsrestrictie niet meer kunnen omzeilen) en iets flexibelere vereisten voor de oudere leeftijdsgroep (zie randnummer 45). De wetgeving zou evenwel een strikte procedure moeten instellen voor het melden van mogelijke inbreuken en het verkrijgen van toestemming. De zelfregulerende uitwerkingen zouden op basis van algemene handhavingsbepalingen in de wet een dwingend karakter moeten kunnen krijgen. Als deze 'Europese COPPA' enige kans op slagen wil hebben, zouden de definities zo breed en zo technologieneutraal mogelijk moeten worden geformuleerd om niet alleen de huidige SNS-aanbieders maar ook alle (zelfs toekomstige) vormen van online diensten en applicaties die op één of andere manier persoonsgegevens verwerken onder de toepassing van de wet te brengen.

Misschien ware het inderdaad beter geweest af te stevenen op een volmaakte Europese wet 'à la COPPA' en op die manier een bredere solide rechtsbasis te verschaffen voor de privacybescherming van jonge SNS-gebruikers. Uit de tekortkomingen en de snel verouderde bepalingen van de Amerikaanse COPPA (zie randnummers 42-43) kan de Europese wetgever immers lessen trekken bij het uitvaardigen van passende regelgeving.

113. Een andere regelgevende optie voor de Europese wetgever zou het uitvaardigen van specifieke SNS-privacywetgeving zijn om de bescherming op SNS in alle EU-lidstaten op één lijn te brengen. Aangezien in de overgang naar het Web 3.0.-tijdperk andere moderne vormen van sociale media en online communicatieplatformen in de toekomst ook bijzondere Europese regels zouden behoeven, is een dergelijke aanpak minder wenselijk. Daarenboven zou deze optie moeilijk te verzoenen zijn met de idee van een co-regulerende strategie en zou deze gespecifieerde regelgeving nog sneller kunnen verwelken dan een kader met algemene gegevensbeschermingsregels. Men dient echter te streven naar voldoende brede en technologieneutrale bepalingen die gericht zijn naar elke dienst die persoonsgegevens verzamelt en/of verwerkt ongeacht het platform waarlangs die gegevens circuleren.

114. Met welk soort wetgevend instrument de EU deze problematiek ook zou reguleren, een efficiënte handhaving van de online privacyregelgeving op zowel Europees als op nationaal niveau blijft een bittere noodzaak. Aangezien bijvoorbeeld Facebook opereert vanuit de Verenigde Staten is internationale samenwerking tussen de politionele en gerechtelijke instanties bovendien onontbeerlijk. Gelet op de opname van het handhavingsluik van het nieuwe EU-voorstel in een aparte richtlijn is handhaving net zoals in andere beleidsdomeinen van de informatiemaatschappij (bijvoorbeeld de intellectuele rechten) een heet hangijzer waarbij een doorgedreven harmonisatie in de EU moeilijk te verwezenlijken is door de terughoudendheid van de Europese wetgever.

Men mag daarenboven niet uit het oog verliezen dat er met betrekking tot de aansprakelijkheid van een tussenpersoon momenteel nog onduidelijkheid heerst over de kwalificatie van een sociale netwerkdienst als 'hosting provider' in de zin van artikel 14 van de Richtlijn Elektronische Handel. Onafgezien van het feit dat er argumenten voorhanden zijn om een sociale netwerkdienst te laten ressorteren onder deze 'safe harbour'-bepaling (zie randnummer 17) dient men de nodige 'tools' te voorzien om een SNS aansprakelijk te stellen in geval van een miskenning van de privacyregels, zeker wanneer minderjarigen hiervan het slachtoffer zijn.

Nu handhaving een belangrijk obstakel blijkt te zijn, kan men ervoor opteren om de nationale (België: CBPL) en/of de Europese privacyautoriteiten (WG 29 en EDPS) naast advies- en controletaken ruimere bevoegdheden toe te kennen w.o. het beslechten van online privacygeschillen ter bescherming van minderjarigen om een efficiënter toezicht op de naleving van de privacybepalingen te bewerkstelligen. Hiervoor zou men zich eventueel kunnen inspireren op de structuur en bevoegdheidspakketten van mediaregulatoren.[244] Het oprichten van een aparte en onafhankelijke nationale toezichtscommissie voor minderjarigen en privacy is tevens een mogelijkheid. Minderjarigen of hun ouders zouden op die manier een klacht kunnen indienen tegen een SNS-aanbieder op grond van een vermeende inbreuk van de privacywetgeving waarop deze privacycommissie de overtreding onderzoekt en een passende sanctie oplegt.

4. Algemeen besluit

115. Het feit dat zowel aanbieders, andere dienstverleners en derdegebruikers op SNS toegang hebben tot een enorme hoeveelheid aan privacygevoelige informatie maakt een online sociaal netwerk een gevaarlijke omgeving voor kinderen en jongeren. Minderjarigen zijn een kwetsbare groep en behoeven een aangepaste privacybescherming op SNS. In een eerste hoofdstuk werden de bestaande privacybepalingen uiteengezet. Ongetwijfeld blijft de fundamentele regel van artikel 8 EVRM een essentiële basis voor de bescherming van de online privacy van het kind. Door de verticale werking van de bepalingen uit het EVRM is er nood aan bijkomende wettelijke garanties. Het EHRM houdt in zijn rechtspraak over artikel 8 EVRM echter wel rekening met de kwetsbare positie van minderjarigen op het internet.

De RBP bouwt verder op artikel 8 EVRM en is nog steeds het kerninstrument in de EU voor de bescherming van persoonsgegevens. De definities en principes in de RBP heeft men willen formuleren op een technologieneutrale wijze opdat nieuwe ontwikkelingen gemakkelijker onder het toepassingsgebied van de richtlijn zouden kunnen vallen, maar in de huidige Web 2.0.-constellatie lijkt de richtlijn toch voorbijgestreefd te zijn. De nieuwe ontwerptekst is minstens in dit opzicht een vooruitgang.

---

[244] Men denke aan de Vlaamse Regulator voor de Media (VRM) dat bij een overtreding van de mediabepalingen een waarschuwing met het bevel de overtreding stop te zetten kan uitvaardigen of een administratieve boete kan opleggen. (Zie: D. VOORHOOF en P. VALCKE (m.m.v. H. CANNIE), *Handboek Mediarecht (3de editie)*, Brussel, Larcier, 2011, 586.)

116. Een opmerkelijke tekortkoming in het kluwen van de bestaande Europese privacyvoorschriften is, anders dan in de Amerikaanse wetgeving, het gebrek aan bijzondere bepalingen ter online bescherming van minderjarigen. De adviesinstanties en de rechtsoverwegingen in de ontwerpverordening duiden op het belang van het kind ex. artikel 3 van het VN-Kinderrechtenverdrag, maar zoals *supra* werd aangegeven mankeert dit internationaal verdrag een juridisch afdwingingsmechanisme waardoor ook artikel 16 van dit verdrag geen solide rechtsbasis kan bieden.

117. De ontwerpverordening van 2012 waarvan de relevante artikelen werden besproken in Hoofdstuk 2 wil tegemoetkomen aan bovenstaande tekortkomingen. De nieuwe tekst tracht de teugels wat strakker aan te spannen door o.a. expliciet een artikel 8 ter bescherming van kinderen onder de dertien jaar te voorzien dat lijkt geïnspireerd te zijn op de bepalingen van de COPPA. Toch lijkt het spectrum van dit artikel te eng te zijn en is er het risico dat de bepaling zal worden omzeild door de limitatief opgesomde toepassingsvoorwaarden. Naast het invoeren van een kind-specifiek artikel heeft de Europese wetgever trachten rekening houden met de complexe SNS-sector en een aantal belangrijke bepalingen ingevoerd zoals 'het recht om vergeten te worden' om SNS-gebruikers meer controle te geven over het online gebruik van hun persoonsgegevens.

De nieuwe en gewijzigde bepalingen in de ontwerpverordening mogen dan wel nog enige bezinning en verduidelijking behoeven naar de mening van de WG 29 en de EDPS, de nieuwe tekst toont aan dat de Europese wetgever het domein ter harte neemt en wil streven naar een diepere en aangepaste harmonisatie en uitwerking van de gegevensbeschermingsregels.

118. Omdat de toepassing van de huidige wetgeving persoonsgegevens-bescherming op de Web 2.0.-realiteit van SNS niet evident is en een strikte overheidsregulering *an sich* niet in staat is de privacy van minderjarigen op SNS ten volle te beschermen, hebben zowel Europese als internationale beleidsinstanties alternatieve regulerende initiatieven genomen. Zo werd in Hoofdstuk 3 uitvoerig aandacht besteed aan de EU-SSNP en de recente Aanbeveling van de Raad van Europa. Een elementaire vereiste voor een voor minderjarigen veilige en transparante SNS-omgeving is dat aanbieders voldoende evenwichtige, gebruiksvriendelijke en leeftijdsaangepaste algemene voorwaarden en privacy-instellingen dienen te voorzien.

Een spijtige vaststelling is dat ondanks de modern geformuleerde en goedbedoelde principes in de soft law-instrumenten een efficiënte naleving niet kan worden verwezenlijkt zonder enige dwingende kernbepalingen. Dit is meteen het grootste defect van het concept van zelfregulering. Co-regulering waarbij op basis van een afdwingbaar wettelijk privacykader en onder het toeziend oog van de overheid aanvullende regels worden uitgewerkt door de SNS-sector lijkt een betere regelgevende strategie te zijn. Enerzijds kan de overheidsinbreng er in bestaan nieuwe regels te formuleren binnen het bestaande gegevensbeschermingskader (zoals op EU-niveau momenteel het geval is),

anderzijds kan geopteerd worden voor een internet- of zelfs SNS-specifiek wetgevend instrument om (althans op korte termijn) het privacyprobleem op SNS aan te pakken. Een *sui generis*-privacyorgaan kan bovendien een forum bieden voor eventuele klachten en SNS-aanbieders sanctioneren wanneer privacyrechten worden miskend. Ten slotte moeten op basis van het wetgevende kader bewustmakingscampagnes, aanbevelingen en 'user empowerment' de betrokken rechtssubjecten blijven informeren en weerbaarder maken tegen een schending van hun persoonlijke levenssfeer. Deze initiatieven bieden ongetwijfeld een 'incentive' opdat jonge gebruikers ook zelf de moeite zouden doen om de algemene voorwaarden en privacyrichtlijnen door te nemen en een schending van hun privacy op SNS te vermijden.

BIBLIOGRAFIE

I. Wetgeving

- **België**

Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, *B.S.*, 18 maart 1993.

Artikel 22 van de Grondwet.

- **Europese Unie**

Richtlijn 95/46/EG betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (‘richtlijn bescherming persoonsgegevens), *Pb.L.* 23 november 1995, afl. 281, 31-50.

Richtlijn 98/48/EG van het Europees Parlement en de Raad van 20 juli 1998 tot wijziging van Richtlijn 98/34/EG betreffende een informatieprocedure op het gebied van normen en technische voorschriften, *Pb.L.* 5 augustus 1998, 18-26.

Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt (‘richtlijn inzake elektronische handel’), *Pb.L.* 17 juli 2000, 1-16.

Beschikking 276/99/EG van het Europees Parlement en de Raad van 25 januari 1999 tot vaststelling van een communautair meerjarenactieplan ter bevordering van een veiliger gebruik van Internet door het bestrijden van illegale en schadelijke inhoud op mondiale netwerken.

Beschikking nr. 1151/2003/EG van het Europees Parlement en de Raad van 16 juni 2003 tot wijziging van Beschikking nr. 276/1999/EG tot vaststelling van een communautair meerjarenactieplan ter bevordering van een veiliger gebruik van internet door het bestrijden van illegale en schadelijke inhoud op mondiale netwerken, *Pb.L.* 1 juli 2003.

Beschikking 2005/854/EG van het Europees Parlement en de Raad van 11 mei 2005 tot vaststelling van een communautair meerjarenprogramma ter bevordering van een veiliger gebruik van het internet en nieuwe online-technologieën.

Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector van elektronische communicatie, *Pb.L.* 31 juli 2002, afl. 201, 37-47.

Richtlijn 2002/21/EG van het Europees Parlement en de Raad van 7 maart 2002 inzake een gemeenschappelijk regelgevingskader voor elektronische communicatienetwerken en -diensten (‘kaderrichtlijn’), *Pb.L.* 24 april 2002, 33.

Richtlijn 2002/20/EG van het Europees Parlement en de Raad van 7 maart 2002 betreffende de machtiging voor elektronische communicatienetwerken en -diensten ('Machtigingsrichtlijn'), *Pb.L.* 24 april 2002, 21.

Richtlijn 2002/19/EG van het Europees Parlement en de Raad van 7 maart 2002 inzake de toegang tot en interconnectie van elektronische communicatienetwerken en bijbehorende faciliteiten ('Toegangsrichtlijn'), *Pb.L.* 24 april 2002, 7.

Richtlijn 2002/22/EG van het Europees Parlement en de Raad van 7 maart 2002 inzake de universele dienst en gebruikersrechten met betrekking tot elektronische communicatienetwerken en diensten ('Universele dienstrichtlijn'), *Pb.L.* 24 april 2002, 51.

Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie

Verordening (EG) nr. 2006/2004 betreffende samenwerking tussen de nationale instanties die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming, *Pb.L.* 18 december 2009, 11-36.

Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009 tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronische communicatienetwerken en –diensten

Richtlijn 2002/77/EG van de Commissie van 16 september 2002 betreffende de mededinging op de markten voor elektronische communicatienetwerken en -diensten ('Mededingingsrichtlijn'), *Pb.L.* 17 september 2002, 21.

Richtlijn 2010/13/EU van 10 maart 2010 betreffende de coördinatie van bepaalde wettelijke en bestuursrechtelijke bepalingen in de lidstaten inzake het aanbieden van audiovisuele mediadiensten ('Richtlijn audiovisuele mediadiensten' of 'AVMD-richtlijn') (gecodificeerde versie).

Voorstel voor een verordening van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (algemene verordening gegevensbescherming, 25 januari 2012, COM/2012/11 definitief. Te raadplegen op: http://ec.europa.eu/justice/dataprotection/ document/review2012/com_2012_11nl.pdf.

- **Raad van Europa**

Verdrag van de Raad van Europa tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens van 28 januari 1981 en het Aanvullend Protocol bij het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens inzake toezichthoudende autoriteiten en grensoverschrijdend verkeer van gegevens van 8 november 2001, te raadplegen op: http://conventions.coe.int/ Treaty/en/Treaties/Html/108.htm.

II. Beleidsdocumenten

- ***Nationaal***

Commissie voor de bescherming van de persoonlijke levenssfeer, advies 38/2002 van 16 september 2002 betreffende de bescherming van de persoonlijke levenssfeer van minderjarigen op internet, 1-10, te raadplegen op: http://www.internet-observatory.be/internet_observatory/pdf/advice_privacy_nl.pdf

Commissie Meijers (Nederland), verslag betreffende het voorstel voor de herziening van de EU-wetgeving bescherming persoonsgegevens, 2 maart 2012, te raadplegen op: http://www.eerstekamer.nl/eu/brief2/20120302/notitie_van_de_commissie_meijers/document3.

- ***Europees***

Europese Unie

Aanbeveling van de Raad van 24 september 1998 betreffende de ontwikkeling van de concurrentiepositie van de Europese industrie van audiovisuele en informatiediensten door de bevordering van nationale kaders teneinde een vergelijkbaar en doeltreffend niveau van bescherming van minderjarigen en de menselijke waardigheid te bereiken, *Pb.L.* 7 oktober 1998, 48-55.

Mededeling van de Commissie aan de Raad, het Europees Parlement, het Economisch en Sociaal Comité en het Comité van de Regio's over de illegale en schadelijke inhoud op internet, COM(96)487.

Tweede evaluatieverslag van de Commissie voor de Raad en het Europees Parlement van 12 december 2003 over de toepassing van de aanbeveling van de Raad van 24 september 1998 over de bescherming van minderjarigen en de menselijke waardigheid, COM(2003)/776, 3.

Verslag van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's over de toepassing van de aanbeveling van de Raad van 24 september 1998 betreffende de bescherming van minderjarigen en de menselijke waardigheid en van de aanbeveling van het Europees Parlement en de Raad van 20 december 2006 betreffende de bescherming van minderjarigen en de menselijke waardigheid en het recht op weerwoord in verband met de concurrentiepositie van de Europese industrie van audiovisuele en online-informatiediensten – Bescherming van kinderen in de digitale wereld, SEC(2011)1043 definitief, te raadplegen op: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM: 2011:0556:FIN:NL:HTML.

Conclusies van de Raad over de bescherming van kinderen in de digitale wereld, C 372/04, 20.12.2011, 15.

Advies van de Europese Toezichthouder voor gegevensbescherming betreffende de mededeling van de Commissie aan het Europees Parlement, de Raad, het

Economisch en Sociaal Comité en het Comité van de Regio's – 'Een integrale aanpak van de bescherming van persoonsgegevens in de Europese Unie', *Pb.C.* 22 juni 2011.

Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's, 'Een integrale aanpak van de bescherming van persoonsgegevens in de Europese Unie', 4 november 2010, COM(2010) 609 definitief.

Commissie van de Europese Gemeenschappen, Europese Governance – Een witboek, 25 juli 2001 (COM)2001 428 definitief, te raadplegen op: http://eur-lex.europa.eu/LexUriServ/site/nl/com/2001/com2001_0428nl01.pdf.

Opinion of the European Data Protection Supervisor on the data protection reform package, 7 maart 2012. Te raadplegen op: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf.

Werkgroep Gegevensbescherming artikel 29, Advies 2/2009 over de bescherming van persoonsgegevens van kinderen (Algemene richtlijnen en het bijzondere geval van scholen), 11 februari 2009, te raadplegen op: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/ wp160_nl.pdf.

Werkgroep Gegevensbescherming Artikel 29, Advies 1/2010 over de begrippen 'voor de verwerking verantwoordelijke' en 'verwerker', 16 februari 2010, te raadplegen op: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_nl.pdf.

'Safer Social Networking Principles for the EU', 10 februari 2009, te raadplegen op:http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf.
Werkgroep Gegevensbescherming Artikel 29, Advies 5/2009 over online sociale netwerken, 12 juni 2009, te raadplegen op: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/ wp163_nl.pdf.

Europees Economisch en Sociaal Comité, Advies van 4 november 2009 over de impact van sociale netwerksites op burgers/consumenten, te raadplegen op: https://toad.eesc.europa.eu/ ViewDoc.aspx?doc...2009_AC_NL.
Article 29 Data Protection Working Party, Opinion 01/2012 on the data protection reform proposals, 23 march 2012, te raadplegen op: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf.

Aanbeveling van het Europees Parlement en de Raad van 20 december 2006 betreffende de bescherming van minderjarigen en de menselijke waardigheid en het recht op weerwoord in verband met de concurrentiepositie van de Europese industrie van audiovisuele en online-informatiediensten, *Pb.L.* 27 december 2006, 72-77.

Raad van Europa

Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profling, 23 november 2010. Te raadplegen op: https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec(2010)13&Language=lanEnglish&Ver=original&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383.

Recommendation CM/Rec(2012)4 of the Committee of Ministers to member States on the protection of human rights with regard to social networking services, 4 april 2012. Te raadplegen op: https://wcd.coe.int/ViewDoc.jsp?id=1929453&Site=CM.

- **Internationaal**

Memorandum van Rome, goedgekeurd op de 30ste Conferentie van commissarissen voor de bescherming van gegevens en de persoonlijke levenssfeer, Straatsburg, 17 oktober 2008, te raadplegen op: http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf.

III. Rechtspraak

EHRM, X. and Y. v. the Netherlands, 26 maart 1985, no. 8978/80. Te raadplegen op: http://www.coe.int/t/dg2/equality/domesticviolencecampaign/resources/x%20and%20y%20v%20the%20netherlands_EN.asp.

EHRM, Mark Rees v. United Kingdom, 17 oktober 1986, *Publ.Hof*, Serie A, Vol.106.

EHRM, Graham Gaskin v. United Kingdom, 7 juli 1989, *Publ.Hof*, Serie A, Vol. 160.

HvJ, 6 november 2003 (C-101/01), Jur. I-12971. (zaak Lindqvist)

US Supreme Court, ACLU v. Mukasey, 22 juli 2008, te raadplegen op: http://epic.org/free_speech/_copa/ACLU_v_Mukasey.pdf)

EHRM, K.U. v. Finland, 2 december 2008, no. 2872/02. Te raadplegen op: http://www.coe.int/t/dghl/standardsetting/dataprotection/Judgments/KU%20v%20Finland%20en%20presse.pdf.

EHRM, 16 december 2010, Aleksey Ovchinnikov v. Rusland, no. 24061/04. Te raadplegen op: http://cmiskp.echr.coe.int/tkp197/viewhbkm.asp?sessionId=72196096&skin=hudocen&action=html&table=F69A27FD8FB86142BF01C1166DEA398649&key=40590&highlight=.

HvJ, 16 februari 2012, SABAM t. Netlog, te raadplegen op: http://www.iept.nl/files/2012/IEPT20120216 HvJEU_SABAM_v_Netlog.pdf

IV. Monografieën

CLARCK, C., 'The answer to the machine is in the machine' in HUGENHOLTZ, P.B. (ed.), *The Future of Copyright in a Digital Environment*, The Hague, Kluwer Law International, 139.

CURTIN, D.M. en PUNT-HEYNING, L.H., *Europese integratie*, Amsterdam, Kluwer, 2006, 30.

DEELSTRA, K., *Handboek Zoekmachinemarketing*, Zutphen, Koninklijke Whörmann, 2008, 384-385.

DIERICKX, L., *Het recht op afbeelding*, Antwerpen, Intersentia, 2005, 4.

DUMORTIER, J., 'Privacybescherming bij de verwerking van persoonsgegevens', in *Mediarecht, Telecommunicatie en telematica*, Mechelen, Kluwer, 1999, Afl. 12, 59-62.

FRACKMAN, A., MARTIN, R.C. en RAY, C., *Internet and Online Privacy: A Legal and Business Guide*, ALM Publishing, 2002, 46

GIESEN, I., *Alternatieve regelgeving en privaatrecht*, Amsterdam, Kluwer, 2007, 30.

LEFEVER, K., LIEVENS, E. en VALCKE, P., 'Alle regels overboord voor mediawijze minderjarigen?' in X. (eds.), *Recht in beweging*. *17de VRG Alumnidag*, Antwerpen, Maklu, 2010, 341-361.

LIEVENS, E., *Protecting Children in the Digital Era. The Use of Alternative Regulatory Instruments*, Leiden en Boston, Martinus Nijhoff Publishers, 2010, International Studies in Human Rights, Vol. 105, 584 p.

LIEVENS, E., VALCKE, P. en STEVENS, D., *Praktijkboek recht en internet. Vrijheid van meningsuiting (Titel II, Hoofdstuk 3)*, Brugge, Vanden Broele, 2005, 77 p.

PARMENTIER, S. (ed.), *De rechten van de mens op het internet*, Antwerpen, Maklu, 2000.

PETERSEN, P., *Handboek Online Marketing*, Amsterdam, Kluwer, 2009, 76 en 80.

VAN BELLEN, A.J.M., *Recht en elektronische handel*, Amsterdam, Kluwer, 2002, 63.)

VAN DIJK, J.A.G.M. De netwerkmaatschappij: sociale aspecten van nieuwe media, Kluwer, 2001, 310 p.

VAN EECKE, P.(ed.), *Recht en elektronische handel*, Brugge, Larcier, 2011, 7.

VAN EJK, N., ASSCHER, L., BERGER, N. en KABEL, J., *De regulering van media in internationaal perspectief*, Amsterdam University Press, 2005, 107 p.

VANDE LANOTTE, J. en HAECK, Y. (eds.), *Handboek EVRM. Deel 2. Artikelsgewijze commentaar (Volume I)*, 2004, Antwerpen, Intersentia, 711.

VERHELLEN, E., *Verdrag inzake de rechten van het kind. Achtergrond, motieven, strategieën, hoofdlijnen*, Antwerpen, Garant, 2000, 80-82.

VERMEULEN, G. (ed.), *Strafrechtelijke bescherming van minderjarigen*, Antwerpen-Apeldoorn, Maklu, 2001, 699 p.

VOORHOOF, D. en VALCKE, P. (m.m.v. CANNIE, H.), *Handboek Mediarecht* (3de editie), Brussel, Larcier, 2011, CIC, 688 p.

WITTEVEEN, W.J., GIESEN, I. en DE WIJKERSLOOTH, J.L., *Alternatieve regelgeving*, Amsterdam, Kluwer, 2007, 25.

V. Bijdragen in tijdschriften

BAUWENS, J., 'Discours over jongeren in de nieuwsmedia. Over 'cool kids' en You Tube Killers', *TJK* 2008/5, 301-306.

BERKVENS, J.M.A., 'Richtsnoeren publicatie persoonsgegevens op internet', *Computerr.* 2008/132, 199.

ANN BUB, K., 'Privacy's role in the discovery of social networking site information', *S.M.U.L. Rev.* 2011, 1435.

BLOK, P.H., 'Privacybescherming in alle staten. Internationaal privacyrecht en IPR onder de Europese Privacyrichtlijn', *Computerr.* 2005/45, 297-304.

BUB, K.A., 'Privacy's role in the discovery of social networking site information', *S.M.U.L. Rev.* 2011, 1433-1462.

CUIJPERS, C.M.K.C., 'Toepasselijk privacyrecht in de wolk', *Computerr.* 2011/3, 115-122.

GROOTHUIS, M., 'Uitspraak EHRM over bescherming van minderjarigen op internet, *Computerr.* 2009, afl. 2, 91.

JACOBSON, P., 'The Child Online Protection Act: Taming the World 'Wild' Web', DePaul-LCA J. *Art and Ent.* L. 421 1998-1999, 421-447.

KINDT, E. 'Mobiliteit in de 21ste eeuw: zwanenzang van het recht op privacy?', *Computerr.* 2010/1, 4.

LIEVENS, E. en DUMORTIER, J., 'Bescherming van minderjarigen online: stand van zaken en blik op de toekomst, *Computerr.* 2005, afl. 2, 59-64.

LIEVENS, E., 'Bescherming van minderjarigen in de informatiemaatschappij: een wettelijk kader (in België?)', *Computerr.* 2004, afl. 3, 163-164.

LIEVENS, E., LEFEVER, K. en VALCKE, P., 'Jongeren en media. Een delicaat evenwicht tussen bescherming en beleving', *TJK* 2008/5, 291-300.

LODDER, A., 'Schadelijke of ongewenste informatie op sociale netwerksites, *Computerr.* 2010, afl. 3, 107-114.

MANI, N.E., 'Judicial scrutiny of congressional attempts to protect children from the internet's harms: will internet filtering technology provide the answer congress has been looking for?', *B.U. J. Sci. And Techn*. L. 201 2003, 201-208.

MATECKI, L.A., 'Update: COPPA is Ineffective Legislation! Next Steps for Protecting Youth Privacy Rights in the Social Networking Era', Northwestern Journal of Law and Social Policy 369 2010, 369 e.v.

NICCOLI, A., 'Least Restrictive Means: a clear path for user-based regulation of minors' acces to indecent material on the internet', *J. Legis* 225 2001, 225-236.

PAS, H., Kinderen en media. Of zou het moeten zijn: media en kinderen?, *TJK* 2008/5, 283-286.

PRINS, C., 'Gelekte voorstellen EU wetgeving betreffende bescherming persoonsgegevens', *Computerr.* 2012/1, 89.

STODDART, J.,'Privacy in the era of social networking: legal obligations of social media sites'*, Sask. L. Rev.* 2011, 263-274.

VALGAEREN, E. en LEITNER, L. 'Smartphones en privacy – Vrienden, vijanden of ergens tussenin?', *Computerr.* 2012/1, 2-9.

VALGAEREN, E., 'SNS en de nieuwe vriendschappen: Narcissus in het kwadraat!', *Computerr.* 2010/3.

VALGAEREN, E., 'Sociale netwerksites – De digitale bijenkorven. Korte inleiding op het themanummer Sociale-netwerksites', *Computerr.* 2010/3, 94-96.

VAN DEN HOVEN VAN GENDEREN, R., 'Sociale netwerken, vloek of zegen? Algemene voorwaarden tot het gebruik van persoonlijke informatie', *Computterr.* 2010/3, 97-106.

VAN DER SLOOT, B. en ZUIDERVEEN BORGESTUS, F.J., 'De amendementen van de Richtlijn Burgerrechten op de e-Privacyrichtlijn', *P & I* 2010/4, 162.

VAN EECKE, P. en TRUYENS, M., 'Privacy en sociale netwerken', *Computerr.* 2010/3, 115-128.

VANDEKERCKHOVE, A. 'Vanuit het kinderrechtencommissariaat. Minderjarigen, media en (gebrek aan) privacy', *TJK* 2008/5, 350-353.

VANZEGBROECK, K, 'Dossier: media en kinderen. Naar een positief en stimulerend mediabeleid voor kinderen', *TJK* 2008/5, 286-290.

VI. Krantenartikels

'Tiener stapt uit leven na pesterijen op Facebook', *DS* 12 januari 2012.

'Lieten: foto's van slachtoffers busongeval publiceren is er ver over', *Knack* 16 maart 2012, te raadplegen op: http://www.knack.be/nieuws/belgie/lieten-foto-s-van-slachtoffers-busongeval-publiceren-is-erverover/article4000068218128.htm.

'Rechter gaf voorbeeldstraf om sociale netwerksites te beschermen', *Knack* 21 september 2011, te raadplegen op: http://datanews.knack.be/ict/nieuws/nieuwsoverzicht/2011/09/21/rechter-gaf-voorbeeldstraf-om-sociale-netwerksites-te-beschermen/article 1195107501639.htm)

''Like'-knop van Facebook is illegaal in Europa', HLN 23 augustus 2011, te raadplegen op: http://www.hln.be/hln/nl/4125/Internet/article/detail/1307999/2011/08/23/Like--knop-van-Facebook-is-illegaal-in-Europa.dhtml.)

VII. Onlinebronnen

'Nieuwe Europese privacyregels relevant voor sociale netwerken', 9 maart 2012, http://www.wisemen.nl/weblog/weblogs/nieuwe-europese-privacyregels-relevant-voor-sociale-netwerken/.

AUSLOOS, J., 'The 'Right to be Forgotten' – Worth Remembering?', 30 november 2011, http://www.law.kuleuven.be/icri/all_pubs.php?action=pubs_staff&staffid=166&where=.

Cyberkids' e-Privacy. Minderjarigen, minder rechten? (Privacy Paper Nr. 4) Department of Communication Studies, University of Antwerp, Antwerpen, 2005, http://www.e-privacy.be/PrivacyPaper4-Cyberkids-e-Privacy.pdf)

DDMA (Dutch Dialogue Marketing Association), 'Reactie op het concept Privacy Verordening', maart 2012, 3, http://ddma.nl/wp-content/uploads/2012/03/DDMA-reactie-concept-EU-Privacy-Verordening-versie-2.pdf.

DE HERT, P., 'Systeemverantwoordelijkheid voor de informatiemaatschappij als positieve mensenrechtenverplichting', http://www.vub.ac.be/LSTS/pub/Dehert/Dehert_371_restricted.pdf.

EDPS Newsletter (N32, maart 2012), http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Newsletters/Newsletter_32_EN.pdf.

Europese Commissie (Persbericht) 'Digitale agenda: sociale netwerken kunnen meer doen om de privacy van minderjarigen te beschermen', 30 september 2011, http://www.europanu.nl/id/vit6g2bgsjwz/nieuws/digitale_agenda_sociale_netwerkenkunnen?ctx=vidymbu7mlv1.

Europese Commissie (Persbericht), 'Digitale Agenda: Coalitie van technologische topbedrijven en media om het internet een betere plek voor onze kinderen te maken, 1 december 2011,

http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/1485&format=HTML&aged=0&language=EN&guiLanguage=en.

Europese Commissie (Persbericht), 'Digitale Agenda: slechts twee socialenetwerksites bieden automatisch privacybescherming voor profiel van minderjarigen', 21 juni 2011, http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/762&format=HTML&aged=1&language=NL&guiLanguage=en.

Europese Commissie, 'Hoe kan een hervorming de burgers meer bescherming geven', http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/2nl.pdf.

Europese Commissie, 'Wat betekenen de nieuwe gegevensbeschermingsregels voor sociale netwerken?', http://ec.europa.eu/justice/data-protection/ document/review2012 /factsheets/3_nl.pdf.

Europese Commissie, 'Online Abuse: Literature Review and Policy Context' (in het kader van het Europese Online Grooming Project), februari 2011, 8. Te raadplegen op: http://www.europeanonlinegroomingproject.com/wp-content/file-uploads/EOGP-Literature-Review .pdf.

FTC, Implementing the Children's Online Privacy Protection Act: A Report to Congress, februari 2007, http://www.ftc.gov/oia/ftccoppareport.pdf.

HOGBEN, G. (ed.), 'Security Issues and Recommendations for Online Social Networks', ENISA Position Paper No. 1, oktober 2007, http://www.enisa.europa.eu/activities/ identity-and-trust/past-work-areas/social-networks/security-issues-and recommendations-for-online-social-networks.

Joint Statement on Key Principles of Social Networking Sites, 8 mei 2008, http://www.state.tn.us/attorneygeneral/cases/facebook/ facebookstatement.pdf.

LIEVENS, E., 'Risk-reducing regulatory strategies for the protection of minors in online social networks', KUL, 28 maart 2011, te raadplegen op: http://www.eurocpr.org/ data/2011/2_Lievens.pdf.

LIEVENS, E., VALCKE, P. en VALGAEREN, P.J., 'State of the art on regulatory trens in media. Identifying whether, what, ho wand who to regulate in social media', ICRI KULeuven, december 2011, 52, http://emsoc.be/2552-conclusions-building-blocks-for-the-creation-of-regulatory-strategies-for-social-media/.

LODDER, A.R., VAN DEN HOVEN VAN GENDEREN, R., ENGELFRIET, A., MEKIC, D. e.a., 'Recht en Web 2.0', *Publicatiereeks NVvIR* No. 27, 2010, http://da.nny.nl/wp-content/uploads/2008/ 05/rechtenweb20. Pdf.

Risks and safety on the internet: The perspective of European children. Full findings and policy implications from the *EU Kids Online* survey of 9-16 year olds and their parents in 25 countries, http://www2.cnrs.fr/sites/en/fichier/rapport_english.pdf.

REDING, V., 'Think before you post! How to make social networking sites safer for children and teenagers?', Speech op de Safer Internet Day, Straatsburg, 9 februari 2010, http://europa.eu/rapid/pressReleasesAction.do?reference =SPEECH/10/22&format=HTML&aged=0&language=EN&guiLanguage=en.

REDING, V., Member of the European Commission responsible for Information Society and Media, 'Digital Europe: the Internet Mega-trends that will Shape Tomorrow's Europe European Internet Foundation, Special Event "A view of the Digital World in 2025",Brussels 13 November 2008, http://europa.eu/rapid/pressReleasesAction.do?reference =SPEECH/08/616.

VOORHOOF, D., 'Recente arresten van het EHRM in verband met artikel 10 EVRM (vrijheid van meningsuiting en informatie)', november- december 2008, /Cms_global/uploads/publicaties/dv/06recente_publicaties_case_law/AM.2009.01.EHRM.NovDec2008.20.04.pdf.

VYNCKE, S., 'Het voorstel voor een Europese Privacy Verordening doorgelicht', http://siriuslegal.wordpress.com/2012/02/06/het-voorstel-voor-een-europese-privacy-verordening-doorgelicht/.

VIII. Websites

http://www.wdmcentral.be/

http://www.legislation.gov.uk/

http://www.law.kuleuven.be

http://economie.fgov.be/

http://www.privacycommission.be/nl/sociale-netwerken

http://www.digitale-media.be/

http://www.kijkwijzer.nl/

http://ec.europa.eu/

http://www.cbpweb.nl/

http://www.wdmcentral.be/

http://www.psw.ugent.be/

http://www.ftc.gov/

http://www.europarl.europa.eu/

http://www.coe.int/

http://economie.fgov.be/

http://epic.org/privacy/kids/.

http://nl.wikipedia.org

http://www.edps.europa. Eu

http://www.enisa.europa.eu/

http://www.datenschutz-berlin.de/

http://ecfr.gpoaccess.gov