

Big Brother in de bib: Privacy in bibliotheken

In tijden van terreur worden mensen toleranter voor de indringing in hun privacy. In Vlaanderen is er vooralsnog geen specifieke anti-terroriswetgeving maar veel Europese landen, waaronder ook Nederland, lieten zich al inspireren door de Amerikaanse Patriot Act. Privacy wordt stilaan een illusie. Ook in de bibliotheek ontsnapt de burger niet aan het alziend oog van Big Brother. Zijn wij bereid om in ruil voor meer 'veiligheid' belangrijke democratische waarden als vrije toegang tot informatie en privacy op het spel te zetten?

Patriot Act

Precies zes weken na de terroristische aanslagen van 11 september 2001 keurde het Amerikaanse Congres, onder grote druk van de toenmalige minister van Justitie, John Ashcroft, een wet van 342 pagina's goed. De USA Patriot Act (Uniting and Strengthening America Providing Appropriated Tools Required to Intercept and Obstruct Terrorism) bevat een arsenaal van anti-terrorisemaatregelen. Er is zo goed als geen noemenswaardige politieke hoorzitting of debat aan het goedkeuren van de wet voorafgegaan. Van een breed maatschappelijk debat was al helemaal geen sprake. Wegens tijdsgebrek brachten verschillende afgevaardigden hun stem uit zonder de tekst grondig te hebben gelezen.

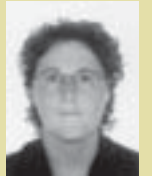
De Patriot Act heeft veel commotie veroorzaakt onder de Amerikaanse bibliothecarissen en bibliotheekmedewerkers. Sommige bepalingen kunnen immers desastreuze gevolgen hebben voor de vrije toegang tot informatie en de privacy van de bibliotheekgebruiker. Het betreft de secties 214 en 215.

Sectie 214

Onder de Patriot Act kan de FBI met een bevelschrift in de hand echt iedereen volgen, waar ze zich ook bevinden en welke telefoon of computer ze ook gebruiken. Dat betekent dat de communicatie die iemand voert vanuit de bibliotheek onderhevig kan zijn aan onderzoek door de FBI. Zodra de FBI vindt dat de data relevant zijn voor een lopend onderzoek, kan hij een bevelschrift krijgen. Er hoeft zelfs geen vermoeden van een misdaad te bestaan.

De FBI kan nu niet alleen telefoonnummers maar ook e-mailheaders en urls van bezochte sites controleren. 'Content' mag niet worden bekeken maar gegevens over het internetverkeer zijn nauwelijks te scheiden van de inhoud. Als je weet welke site iemand bezocht heeft, weet je ook wat hij daar gelezen heeft. Als je de headers van een e-mail bekijkt, weet je door het lezen van de onderwerpregel al waar de inhoud van de mail over gaat.

Isabel Van Ackere is leerkracht Italiaans aan het CVO Sint-Paulus te Waregem
isabel_bologna@hotmail.com



Sectie 215

Sectie 215 geeft de FBI het recht om records van bedrijven, boekhandels en bibliotheken te doorzoeken. Wat betreft de bibliotheken gaat het om de leengegevens of om de gegevens die de bibliotheek bijhoudt over het gebruik van internet-terminals. Er is wel een bevelschrift vereist maar de rechter is verplicht zijn handtekening te zetten als de overheid beweert dat ze met een onderzoek naar terrorisme bezig is.

Een onderzoek naar het leen- of surfgedrag van iemand kan plaatsvinden zonder dat die persoon daarvan op de hoogte wordt gebracht. De bibliotheekmedewerkers zijn bovendien tot geheimhouding verplicht. Het is dan ook bijzonder moeilijk om na te gaan in welke mate sectie 215 al werd gebruikt.

Nederland

Ook in Nederland komt de privacy onder druk te staan en zijn er heel wat maatregelen genomen ter verruiming van de bevoegdheden van opsporingsdiensten. De Tweede Kamer heeft op 2 november 2004 het voorstel met de naam 'Wijziging van het Wetboek van Strafvordering en enkele andere wetten in verband met de regeling van bevoegdheden tot het vorderen van gegevens' aangenomen. Ondanks herhaalde protesten van de Federatie van Organisaties in het Bibliotheek-, Informatie-, en Documentatiewezen

(FOBID) heeft de Eerste Kamer op 5 juli 2005 dit voorstel tot wet gemaakt. Door die wet kunnen bibliotheken worden verplicht gegevens over gebruikers te verstrekken. Naar analogie van de Patriot Act moet er zelfs geen sprake zijn van concrete verdenkingen. Deze wet legt dan ook de basis voor een algemene informatieplicht, een algemeen toezicht op alle burgers.

Vlaanderen

Hoe is de situatie in Vlaanderen? Er verschijnt in de Vlaamse media sporadisch wel eens een artikel over de Patriot Act maar dat is dan meestal een heel algemeen artikel dat zich beperkt tot de Amerikaanse situatie. De Vlaamse bibliotheek- en informatiewereld hult zich in stilte. Blijkbaar heerst de overtuiging dat het in Vlaanderen nooit zover zal komen.

In tegenstelling tot Nederland beschikt Vlaanderen wel over een standpuntverklaring over vrije toegang tot informatie. Ze werd opgesteld door de VVBAD en dateert van 1998¹. Of de principes in deze verklaring ook leven in de praktijk is een andere zaak.

Het Vlaams Centrum voor Openbare Bibliotheken (VCOB) organiseert sinds april 2002 discussiefora voor openbare bibliotheken. Bij wijze van experiment hebben we in april 2005 in de zoekmachine van die fora de termen 'privacy' en 'patriot' ingetikt. De zoekopdracht met de term 'privacy' geeft welgeteld één resultaat. Het gaat om een vraag of er in het bibliotheekreglement een privacyclausule opgenomen moet worden. Elke professionele organisatie die persoonsgegevens verwerkt moet de bij wet vastgelegde spelregels volgen. Het is verontrustend dat dit niet voor iedereen in het werkveld evident is.

De zoekopdracht met de term 'patriot' levert tot onze verbijstering helemaal niets op. We besloten dan ook om zelf een bericht te posten op het discussieforum 'bibliotheekmanagement'. Onze vraag was of de bibliotheek recent de politie of het gerecht op bezoek heeft gehad om informatie (leengedrag/surfgedrag) over gebruikers op te vragen. Of zij daarvoor een bevelschrift hadden en of de bibliotheek ook zonder bevelschrift de gevraagde informatie heeft verschaft. Er kwamen in totaal achtenzestig reacties. Vijfenvijftig bibliothecarissen/bibliotheekmedewerkers hadden nog nooit met een dergelijke vraag naar informatie over gebruikers te maken gehad. Dertien herinnerden zich wel een of twee voorvallen. Meestal ging het om een vraag in het kader van een gerechtelijk onderzoek naar moord, drugs...

Slechts één bibliothecaris heeft de speurders bij een vraag naar informatie op het recht op privacy gewezen! Voor de anderen was een uniform of een legitimatiebewijs al voldoende om de speurders ter wille te zijn. Wie verdacht wordt van een strafbaar feit heeft blijkbaar geen recht meer op privacy. Gezien het beperkte aantal respondenten kunnen we bezwaarlijk van een wetenschappelijk ver-

Enkele reacties

"Het zou niet bij me opkomen om te vragen of de politie daar een machtiging toe heeft, als de politie zoiets vraagt, dan geven wij gewoon antwoord."

"In geen enkel geval was er zoiets als een huiszoekingsbevel, maar ik kan je verzekeren dat als er plots een paar politiemannen in burger met legitimatie voor je staan, dat dit niet het eerste is waar je aan denkt. We zijn immers goed in de reflex om zo juist en eerlijk mogelijke antwoorden te geven op informatievragen."

"In het algemeen zie ik eigenlijk geen problemen om aan de politie alle informatie te geven die we materialiter kunnen geven indien zij dat in het kader van een onderzoek nodig hebben. Ik ga er van uit dat zij dat niet lichtvaardig vragen."

"De politie is hier toen 1 keer geweest om het surfgedrag na te gaan van een klant die als vermist was opgegeven. Ze hadden geen bevel tot huiszoeking. Wij hebben hen dat wel toegelaten... Het ging om een klant die alleen kwam surfen en die ons al verschillende keren last had berekend. We wisten dat hij 'niet zuiver' was."

"We hebben in verband met een welbepaalde lener reeds tweemaal vragen gehad in verband met het gebruik van internet. We hebben zonder gerechtelijk [sic] bevel de nodige informatie verschaft."

"Een paar jaar geleden kregen wij 2 politieagenten op bezoek die wilden weten welke lezers er reeds die dag met onze internetcomputers hadden gewerkt. Ze wilden niet zeggen naar wie of naar wat ze precies op zoek waren. Een gerechtelijk bevel hadden ze niet. Wij hebben onze lijst met namen van personen die die dag reeds met internet hadden gewerkt aan hen getoond."

antwoorde steekproef spreken. Ons onderzoek bleef ook beperkt tot de categorie van de openbare bibliotheken. Wie wel al te maken gehad heeft met een vraag van de politie of het gerecht, is niet geïnformeerd over hoe op dergelijke vragen gereageerd moet worden en welke rechten de bibliotheekgebruikers hebben.

Parlementslid Francis Van den Eynde heeft in april 2005 de volgende vraag gesteld aan de minister van Justitie en de minister van Binnenlandse Zaken: *"In de zogenaamde 'Patriot Act', de anti-terrorismewet die de Amerikaanse regering na 11 september 2001 snel door het Congres drukte, wordt onder meer bepaald dat politie- en veiligheidsdiensten bibliotheekgegevens (met andere woorden de leestlijst) van mensen die ze als verdacht beschouwen, mogen opvragen. 1. Gebeurt het dat bij ons politie- en veiligheidsdiensten gelijkaardige gegevens verzamelen? 2. Zo ja, in welke gevallen en met welk doel?"*

Het antwoord van de minister van Justitie luidde: *"Deze praktijk is niet toegestaan uit hoofde van de Veiligheid van de Staat ten overstaan van ons juridisch kader, wegens het evenwicht dat moet bestaan tussen de fundamentele vrijheden, enerzijds, en het veiligheidsbeleid, anderzijds."* Het antwoord van de minister van Justitie strookt niet met de bevindingen van onze beperkte rondvraag.

De minister van Binnenlandse Zaken gaf als antwoord: *"1. Na contact te hebben genomen met verschillende politiediensten en bibliotheken blijkt dat voor het opvragen van bibliotheekgegevens er zich nog geen geval heeft voorgedaan. Er bestaat in de Belgische wetgeving geen wettelijke basis om deze gegevens op te vragen. De databanken van bibliotheken zijn immers beschermd door de wet op de bescherming van de persoonlijke levenssfeer. Ook bij de bibliotheken stelt zich een probleem. Veel bibliotheken houden de leetuurlijst niet bij, anderen wel maar enkel voor intern gebruik. Voor de veiligheidsdiensten, dien ik te verwijzen naar mijn collega de minister van Justitie. Ook voor verdere details in verband met de wet op de bescherming van de persoonlijke levenssfeer en de eventuele opvraging in het kader van een gerechtelijk onderzoek verwijs ik naar mijn collega de minister van Justitie. 2. Geen gekende gevallen."*

Inbreuken op de privacy

Uitleenadministratie

In de traditionele niet-geautomatiseerde bibliotheek was het bijna onmogelijk na te gaan wie wat gelezen had. Wanneer een lezer een boek leende, werd de boekkaart voor de duur van de uitleening in het lenersmapje gestopt. Bij het inleveren van het boek werd de koppeling lener-boek ongedaan gemaakt door de boekkaart uit het lenersmapje te halen en terug in het boek te stoppen. Om te kunnen nagaan hoeveel keer een bepaald boek werd uitgeleend, werd het nummer van de lenerskaart vermeld op de boekkaart. Met dit systeem kon wel worden nagegaan wie bepaalde 'subversieve' boeken had gelezen. Maar om te controleren welke boeken een specifieke lener gelezen had, zouden in principe alle boeken uit de rekken moeten worden gehaald om de boekkaarten te bekijken. Onbegonnen werk natuurlijk.

In de traditionele bibliotheek zochten gebruikers informatie in een catalogus met steekkaarten of door te grasduinen in de rekken. Op die manier lieten ze geen enkel spoor na van hun zoekgedrag. Als we de observatie door en de interactie met het bibliotheekpersoneel terzijde laten, kunnen we stellen dat de bibliotheekgebruiker in een niet-geautomatiseerde bibliotheek volledige privacy genoot.

In een op technologie gebaseerde bibliotheek is dat wel even anders. In een geïntegreerd systeem wordt de lenersdatabank gekoppeld aan de materialendatabank. Het is technisch perfect mogelijk om bij te houden welke materialen iemand in de loop van de jaren heeft uitgeleend. De meeste softwaresystemen zijn echter zo ingesteld dat de bibliotheekmedewerkers enkel kunnen nagaan wat iemand op een bepaald moment heeft uitgeleend. Zodra de materialen worden teruggebracht, wordt de koppeling verbroken. Specialisten kunnen echter zogenaamde 'gewiste' gegevens weer bovenhalen. Met een gerechtelijk bevel kan de softwareleverancier gedwongen worden om uitleengegevens

aan het gerecht door te geven. Bij een gericht onderzoek kan de bibliotheek uitleengegevens vrijgeven. Een 'fishing operation', zoals mogelijk geworden is onder de Patriot Act, mag de bibliotheek absoluut niet toestaan.

Er wordt ook bijgehouden wie als laatste een specifiek boek, cd... heeft uitgeleend. Dit om bij schade aan de materialen de kosten te kunnen verhalen op die lener. Op basis van uitleengegevens en het zoekgedrag van gebruikers kunnen lezersprofielen gegenereerd worden. Die kunnen dienen om de gebruikers te attenderen op materialen die hen mogelijk interesseren. De Amerikaanse internetboekhandel Amazon past dit systeem al jaren toe.

Technisch is het mogelijk om profielen van lezers aan te maken en die gegevens door te verkopen aan commerciële organisaties, maar de Belgische privacywetgeving laat dit niet toe. Het is evenmin toegestaan om profielen aan te maken voor intern gebruik tenzij de betrokkene zijn expliciete toestemming geeft.

Dit heeft consequenties voor de vrijstelling van aangifteplicht waarvan bibliotheken krachtens art. 55 van de privacywet genieten als ze zich beperken tot zuivere leneradministratie. Die vrijstelling van aangifte vervalt indien lezersprofielen met betrekking tot geïdentificeerde personen worden aangeemaakt. Wat betreft het sturen van (e-)nieuwsbrieven geeft de Commissie voor de Bescherming van de Persoonlijke Levenssfeer het volgende advies: *"Het opsturen van een nieuwsbrief naar de leden van de bibliotheek kan daarentegen, als inbegrepen in het doeleinde van klantenbeheer worden beschouwd, indien deze informatie de activiteiten van de bibliotheek betreft. De toestemming van de betrokken persoon moet ondubbelzinnig zijn maar moet niet noodzakelijk schriftelijk zijn."*² Nieuwsbrieven met op maat gesneden informatie zijn dan weer een andere zaak.

In Nederland gaan er stemmen op om rationeler te gaan collectioneren op basis van uitleengegevens. Onderzoeker Jaap Boter: *"Ik sta er van te kijken dat uitleengegevens nogal eens worden gewist als een lener zijn materialen heeft teruggebracht. Zo gaat veel managementinformatie verloren. Vaak krijg ik dan misplaatste argumenten te horen over de privacy van klanten."*³

Volgens de Belgische privacywetgeving mogen uitleengegevens verwerkt worden op voorwaarde dat ze worden geanonimiseerd.

Internettoegang

Ongeveer 90% van de Vlaamse openbare bibliotheken zijn met het internet verbonden via BibNET. Dit netwerk met een gemeenschappelijke internettoegang wordt beheerd door het VCOB en gerund door de netwerkprovider Ardatis. Als provider is dit bedrijf wettelijk verplicht om de logging van het internetverkeer te verzekeren. Het logt IP-adressen van de

bibliotheken en de bezochte sites. In principe kan dus geen verband gelegd worden tussen een individuele gebruiker in de bibliotheek en zijn surfgedrag, enkel tussen de bibliotheek en het surfgedrag van het collectief van gebruikers.

Bij een vraag van de Federal Computer Crime Unit (FCCU) kan Ardatis enkel zeggen in welke bibliotheek naar een bepaalde site werd gesurft. De Belgische providers moeten volgens de wet van 28 november 2000 inzake informaticacriminaliteit de gegevens van het internetverkeer van hun klanten 12 maanden bijhouden.

Wat te denken van het volgende scenario? Speurders combineren de gegevens van de provider met de registratielijsten van het gebruik van internetcomputers en de tapes van camerabewaking. Op die manier wordt het mogelijk elke beweging van de internetgebruiker in cyberspace te traceren zonder zijn medeweten.

Welke houding nemen we aan tegenover filtersoftware in het licht van het principe van vrije toegang tot informatie? Iedereen is het erover eens dat kinderen afgeschermd moeten worden van bepaalde sites. Maar is dergelijke software geen inbreuk op de privacy van volwassenen?

E-mail

Vergeleken met andere vormen van communicatie, is e-mail nauwelijks beveiligd. Nog voor een bericht zijn eindbestemming bereikt, kan het onderschept worden door hackers. De mailersoftware houdt een log bij van de afzender en de geadresseerde van de e-mail, het tijdstip van ontvangst van de e-mail, en het IP-adres van de computer van waar de e-mail werd verzonden. Een e-mail die verwijderd werd, kan nog opgeslagen zijn in de archieven van de provider. Gelezen en verstuurd e-mail vanaf een pc wordt meestal ook bewaard op die pc. Internettijnen kunnen 'afgeluisterd' worden en zo kan de inhoud van een e-mail onderschept worden. Sommige gratis e-mailproviders, zoals Gmail van Google, scannen automatisch de e-mail en trachten bepaalde trefwoorden te ontdekken om de interesses te kennen. E-mail is dus allesbehalve privé. Alles wat iemand in een e-mail schrijft, kan onderhevig zijn aan onderzoek door de gerechtelijke diensten. De gebruiker van e-mail moet zich ervan bewust zijn dat e-mail zo privé is als een briefkaart. Als hij dan toch vertrouwelijke informatie wil versturen, gebruikt hij beter een programma om het bericht te coderen. Voor iemand met minder goede bedoelingen is mailen van op een computer in de bibliotheek al iets anoniemer. De laatste jaren waren er verschillende incidenten rond haat-



mails en/of dreigmails die vanuit openbare bibliotheken verstuurd werden naar politici. Kort na de moord op Pim Fortuyn in mei 2002, stuurde iemand vanuit de bibliotheek van Eindhoven een e-mail met doodsbedreigingen naar de Groen-Links politica Femke Halsema.

Wie anoniem een e-mail wil versturen, kan onder een valse naam een e-mailadres aanmaken bij een webge-

baseerde e-maildienst zoals Hotmail, Yahoo of Gmail. Om te vermijden dat de gerechtelijke diensten aan de hand van het IP-adres kunnen traceren van wie het bericht komt, kan iemand met minder goede bedoelingen gebruikmaken van een internetcomputer in de bibliotheek. De provider kan de gerechtelijke diensten wel vertellen uit welke bibliotheek het bericht komt maar niet welke gebruiker erachter zit. Zoals vermeld kunnen de speurders toch nog de zender van het bericht identificeren als ze de gegevens van de provider combineren met internetregistratielijsten en tapes van camerabewaking.

Wat betreft de privacy van het bibliotheekpersoneel, is er sinds 26 april 2002 CAO nr. 81 tot bescherming van de persoonlijke levenssfeer ten opzichte van de controle op de elektronische on-linecommunicatiegegevens⁴.

Copyright

Vrije toegang tot informatie is in een democratie van essentieel belang. De toegang tot digitale informatie staat echter onder druk. Uitgevers en auteurs willen hun rechten veilig stellen en zoeken naar methoden om hun inkomsten te garanderen. Er zijn mogelijkheden om het copyright van elektronische informatie technisch te beschermen. Die technologieën worden Electronic Copyright Management Systems (ECMS) of ook wel Digital Rights Management Systems (DRMS) genoemd.

Via DRM-toepassingen kan niet alleen worden aangegeven wie de content kan gebruiken, maar bijvoorbeeld ook wanneer en/of hoe vaak. Het is zelfs mogelijk te bepalen welke handelingen (printen, kopiëren...) met de content zijn toegestaan.

Maar om dit alles te bereiken moeten de gebruikers persoonlijke gegevens verstrekken. Die worden wel 'gecodeerd' met Privacy Enhancing Technologies (PET) zoals encryptie, maar als de sleutels bij de leverancier van de digitale informatie blijven, dan is de bescherming van de privacy van de gebruiker een kwestie van vertrouwen. Het deponeren van de sleutels bij onafhankelijke derden kan een oplossing bieden.

Cameratoezicht

De meeste mensen liggen er niet wakker van, maar camera-bewaking kan een ernstige inbreuk vormen op de privacy. Denken we opnieuw aan de combinatie van loggegevens, internetregistratielijsten en camerabewaking. Als de beelden van camerabewaking niet worden opgeslagen, gaat het niet om verwerking van gegevens en is er geen registratieplicht. Zodra de beelden opgenomen en bewaard worden en de personen op de tapes geanalyseerd worden, geldt wel de registratieplicht. Het publiek moet ingelicht zijn dat er beelden worden opgenomen en weten waarom dat gebeurt. Opnames maken in het geheim is niet toegestaan.

Inlichtingenwerk

Ook bij het inlichtingenwerk moet de privacy van de bibliotheekgebruiker gerespecteerd worden. Mensen stellen niet altijd een gerichte vraag. Ze hebben vaak moeite om een vraag naar informatie helder te verwoorden. Soms stellen ze een vraag in algemene termen terwijl ze eigenlijk naar iets specifiek op zoek zijn omdat het om een delicaat of gevoelig onderwerp gaat zoals echtscheiding of ziekte. Willen wij per se de juiste vraag en context achterhalen omdat wij informatievoorziening als een kerntaak van ons beroep zien? Ook als dat ten koste gaat van de privacy van de gebruiker?

Bescherming van de privacy

Welke maatregelen kunnen bibliothecarissen nemen om de privacy van de gebruikers beter te beschermen? Ten eerste moeten ze op de hoogte zijn van de wetgeving over privacy en computercriminaliteit. Ze moeten elektronische informatie op dezelfde manier behandelen als gedrukte informatie en een gerechtelijk bevel eisen vóór ze gegevens vrijgeven. Ze moeten nooit vrijwillig meewerken. Bibliotheekmedewerkers sturen de gerechtelijke instanties altijd naar de bibliothecaris.

Ten tweede moeten bibliothecarissen beseffen dat alle informatie die ze verzamelen toegankelijk is voor derden. Gegevens die met een bepaald doel verzameld zijn, zoals de laatste lener van een boek, kunnen gebruikt worden voor een minder eerbaar doel. Softwaresystemen mogen niet méér informatie verzamelen dan nodig is om de bibliotheek efficiënt te runnen. Gegevens die niet meer nodig zijn, worden best gewist. Dan kunnen ook niet meer doorgegeven worden.

Ten derde kan de technologie gebruikt worden om de privacy beter te beschermen. Met programma's als Acronis Provac Expert Suite 8.0 kunnen programma's die gebruikers geïnstalleerd hebben, cookies of andere informatie die ze zouden kunnen identificeren, gewist worden. Zelfbedieningsbalies kunnen de privacy bij het uitleenen vergroten.

Ten vierde is het essentieel dat de gebruikers ervan op de hoogte zijn dat de bibliotheek hun privacy niet in alle

omstandigheden kan garanderen. Geef ze tips over hoe ze zelf hun privacy beter kunnen beschermen. Stippel een beleid uit over privacy en het gebruik van het internet in de bibliotheek. Stel een document op dat ter beschikking ligt van de gebruikers. De nieuwe privacywet voorziet in de mogelijkheid voor beroepsverenigingen of organisaties die werken aan een privacybeleid of die een gedragscode wensen te formuleren (te wijzigen of te verlengen), dit voor te leggen aan de privacycommissie⁵.

Besluit

We hebben in Vlaanderen vooralsnog niet te maken met Amerikaanse toestanden maar wat niet is kan nog komen. Amerika is op vele vlakken een trendsetter. Vroeg of laat wordt privacy in bibliotheken ook in Vlaanderen een heet hangijzer. In plaats van achter de feiten aan te hollen en pas te reageren als het kalf al verdrongen is, kan de sector zich beter nu al informeren en maatregelen treffen. Privacy mag dan steeds meer een illusie worden, toch we moeten blijven ijveren voor de bescherming ervan.

Noten

1. VVBAD, *Vrije toegang tot informatie, ook in een digitale omgeving: de rol van bibliotheken*, in: *Bibliotheek- & archiefgids*, (1998) 3: p. 87-90.
2. Michel Parisse, *voorzitter van de Commissie*, in een brief van 1 april 2005.
3. Wendy de Graaff, *Onderzoeker Jaap Boter: Een supermarkt plaatst zijn producten toch ook niet alfabetisch*, in: *Bibliotheekblad*. 6 (2002) 15/16: p. 23.
4. *De volledige tekst van CAO nr. 81 is te vinden op de website van de privacycommissie: <http://www.privacy.fgov.be>.*
5. Art. 44, lid 2 en 3 van de Wet van 8 december 1992 ter bescherming van de persoonlijke levenssfeer ten aanzien van de verwerking van persoonsgegevens zoals gewijzigd door de Wet van 11 december 1998.

SAMENVATTING

De overheid heeft in tijden van angst en terreur de neiging de controle op het doen en laten van haar burgers te verscherpen. Ook de bibliotheek ontsnapt niet aan het alziende oog van Big Brother. In een geautomatiseerde bibliotheek zijn de mogelijke schendingen van de privacy van de gebruikers legio. Zijn de Vlaamse bibliothecarissen zich daar wel van bewust? Zijn ze op de hoogte van de privacywetgeving en de toepassing ervan op de bibliotheeksector? Welke maatregelen kunnen zij nemen om de privacy van de gebruikers beter te beschermen?

ABSTRACT

In times of fear and terror, the government is inclined to tighten up control over her citizens. Big Brother watches them also in the library. In a library based on technology the possible violations of the patron's privacy are countless. Are the Flemish librarians aware of this? Are they well informed about the privacy legislation and the consequences for libraries? What measures can they take to protect their patron's privacy?