Waarop moet je letten als je gratis wifi aanbiedt?

Joris Deene

Menig bibliotheek of archief biedt haar bezoekers draadloos internet (wifi) aan. Het opzetten van een dergelijk draadloos netwerk voor bezoekers roept veel vragen op. Moet je de identiteit van de bezoekers vragen? Ben je aansprakelijk voor wat de bezoekers doen via de internetverbinding? Valt het aanbieden van gratis wifi onder de strenge regels van de Wet elektronische communicatie? Kun je sites monitoren en blokkeren, en is dit onder de privacywetgeving wel toegelaten? Deze bijdrage geeft een antwoord op deze vragen.

AANSPRAKELIJKHEID

De belangrijkste vraag van veel aanbieders van draadloos internet is of ze aansprakelijk zijn als er illegale handelingen gebeuren via de door hen geleverde wifiverbinding. Het antwoord is in de meeste gevallen negatief. Als de aanbieder een louter passieve rol speelt draagt hij geen aansprakelijkheid (art XII.17 *Wetboek Economisch Recht*).

Om niet aansprakelijk te zijn voor het doorgeven van informatie middels het verschaffen van toegang tot een communicatienetwerk is het belangrijk dat de aanbieder van het netwerk geen initiatief neemt om de informatie door te geven, niet bepaalt aan wie de informatie doorgegeven wordt en de informatie niet selecteert of wijzigt. Dit principe werd door het Europees Hof van Justitie bevestigd in een arrest van 15 september 2016 (C-484/4) in een procedure tussen bedrijfsleider McFadden en Sony Music. McFadden stelde in zijn winkel gratis en anoniem toegang tot het internet ter beschikking van zijn klanten. Een gebruiker steelde via het netwerk muziek online. Sony Music eiste een schadevergoeding van McFadden. Het Hof van Justitie oordeelde dat dat niet kon: de aanbieder van een netwerk is slechts een doorgeefluik. Hij oefent geen invloed uit en neemt geen initiatief bij de doorgifte van informatie. Hij kan dus niet veroordeeld worden tot een schadevergoeding.

Het Hof stelt wel dat een rechtbank de aanbieder van een netwerk wel kan opleggen om de inbreuk op het auteursrecht te beëindigen of te voorkomen. Zo kan de rechtbank de aanbieder opleggen om het netwerk te beveiligen met een wachtwoord waarbij gebruikers verplicht zijn hun identiteit op te geven om het wachtwoord te krijgen.

PRIVACY

Dit brengt ons bij de volgende vraag. Kan een instelling het internetverkeer van haar bezoekers monitoren, loggen en controleren? Dat heeft immers een impact op de privacy van die bezoekers. Het monitoren en controleren van internetverkeer houdt het verwerken van persoonsgegevens in, waarop de Algemene Verordening Gegevensbescherming (GDPR) van toepassing is. Volgens de GDPR mogen persoonsgegevens enkel verwerkt worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Het monitoren van het internetverkeer van bezoekers zonder enige motivering is dus uitgesloten.

Er moet bovendien een rechtmatige grondslag zijn voor de gegevensverwerking. De GDPR geeft een limitatieve lijst van grondslagen, waaronder deze drie. Ten eerste is het monitoren mogelijk mits toestemming van de bezoeker. Die toestemming moet vrij, specifiek, geïnformeerd en ondubbelzinnig zijn. Bezoekers moeten dus duidelijk weten dat ze hun toestemming geven voor het monitoren en controleren van hun internetverkeer, bv. om controle uit te oefenen wanneer er aanwijzingen zijn van misbruik. De bezoeker kan de toestemming weigeren, maar de aanbieder kan dan uiteraard de toegang tot het netwerk weigeren.

Ten tweede kan het verwerken van persoonsgegevens noodzakelijk zijn voor de uitvoering van een overeenkomst waarbij de bezoeker partij is. Men kan immers argumenteren dat gebruikers

door in te loggen ingaan op het aanbod van gratis wifi, waardoor er een overeenkomst tot stand komt. In dat geval is het monitoren van het internetverkeer noodzakelijk voor de uitvoering van de overeenkomst als het leveren van een veilig en betrouwbaar netwerk deel uitmaakt van de overeenkomst.

Tot slot is monitoren van het wifinetwerk mogelijk als de verwerking van persoonsgegevens noodzakelijk is voor de behartiging van de gerechtvaardigde belangen van de aanbieder. Het Hof van Justitie oordeelde in een arrest van 19 oktober 2016 (C-582/14) dat het opslaan van persoonsgegevens (in casu IP-adressen) toegelaten is om een website te beschermen tegen cyberaanvallen. Ook bij het beschermen van het wifinetwerk geldt een dergelijk gerechtvaardigd belang.

Bezoekers moeten in ieder geval, ongeacht de grondslag, geïnformeerd worden over de gegevensverwerking. Dat gebeurt meestal via een privacyverklaring. Bovendien moet je bij het monitoren en controleren van het internetverkeer steeds rekening houden met het principe van proportionaliteit en subsidiariteit. Dit houdt in dat het monitoren van het internetverkeer zoveel mogelijk anoniem moet gebeuren. Alleen in geval van klachten of concrete aanwijzingen kun je een specifieke bezoeker controleren.

In plaats daarvan kun je als aanbieder bepaalde websites of diensten automatisch filteren of blokkeren. In dat geval worden bezoekers niet gemonitord of gecontroleerd en is de GDPR niet van toepassing.

GEBRUIKERSVOORWAARDEN

Kan een instelling haar aansprakelijkheid beperken tegenover gebruikers die eventueel schade lijden door het gebruik van een wifinetwerk (bv. door virussen)? Dat kan, als ze gebruikersvoorwaarden oplegt waarbij de gebruiker akkoord gaat dat de aansprakelijkheid van de aanbieder sterk beperkt wordt. Hou wel rekening met de vrij strenge consumentenwetgeving, die zeer kritisch is tegenover het beperken van aansprakelijkheid tegenover consumenten. Anderzijds kun je argumenteren dat bij het aanbieden van een gratis wifinetwerk deze inperking te rechtvaardigen is.

Zorg er wel voor dat de gebruiksvoorwaarden correct aanvaard worden, zodat ze juridisch tegenstelbaar zijn aan de gebruikers. De gebruiksvoorwaarden moeten aan de gebruikers bekendgemaakt worden vooraleer ze gebruikmaken van het wifinetwerk en moeten uitdrukkelijk aanvaard worden. Zorg er ook voor dat gebruikers deze voorwaarden kunnen opslaan of afdrukken.

WET ELEKTRONISCHE COMMUNICATIE

Het aanbieden van elektronische communicatienetwerken valt in principe onder de Wet van 13 juni 2005 betreffende elektronische communicatie. Die wet bepaalt dat wie openbare netwerken aanbiedt zich moet aanmelden bij het Belgisch Instituut voor Postdiensten en Telecommunicatie (BIPT). Er moet aan allerlei eisen voldaan worden, zoals het identificeren van de gebruikers, het bewaren van gegevens en het samenwerken met de gerechtelijke overheden en de inlichtingen- en veiligheidsdiensten. In principe, want deze regels zijn enkel van toepassing op aanbieders van openbare netwerken. Daarvan is pas sprake wanneer iedereen, zonder nadere eisen (behalve eventueel betaling) toegang krijgt tot het internet. Wanneer de toegang beperkt wordt tot een duidelijk afgebakende groep, zoals de bezoekers van een bibliotheek of archief, is er geen sprake van een openbaar netwerk.

Tot slot is het principe van netneutraliteit (vervat in de Europese Verordening 2015/212) niet van toepassing op dergelijke aanbieders. Hierdoor kan de toegang tot bepaalde websites of applicaties verboden worden. Het gebruik van bijvoorbeeld Spotify of Netflix kan dus beperkt worden. ▮▮