Onder een vergrootglas: Onderzoek naar de ervaringen van Nederlandse onderzoeksjournalisten met overheidssurveillance en de impact daarvan op de journalistieke bescherming van vertrouwelijke bronnen

IJzerman, Nikki

Onder een vergrootglas

Onderzoek naar de ervaringen van Nederlandse onderzoeksjournalisten met overheidssurveillance en de impact daarvan op de journalistieke bescherming van vertrouwelijke bronnen

Universiteit Leiden

Nikki IJzerman
s3667332
ijzemannikki@gmail.com

Universiteit Leiden
MA Journalistiek en Nieuwe Media
2022-2023

Masterscriptie

Scriptiebegeleider: Dr. A.R.J. Pleijter
Tweede lezer: Dr. M.P.A. Opgenhaffen

1 augustus 2023

Samenvatting

De onthullingen van Edward Snowden over grootschalige spionage door Amerikaanse inlichtingendiensten hebben vanaf 2013 geleid tot een enorme hoeveelheid nieuwe literatuur over dit onderwerp. Een aanzienlijk deel daarvan gaat over de impact van (digitale) overheidssurveillance op het werk van journalisten en hun omgang met vertrouwelijke bronnen. Dit onderzoek is een aanvulling op de overwegend Amerikaanse literatuur die al beschikbaar is. Aan de hand van semigestructureerde diepte-interviews met tien Nederlandse onderzoeksjournalisten is onderzocht hoe zij de dreiging van overheidssurveillance ervaren en op welke manier dit de omgang met vertrouwelijke bronnen beïnvloedt. Waar in theorie bij journalisten en bronnen een *chilling effect* kan optreden, is daar in dit onderzoek geen bewijs voor gevonden. Wel blijkt uit de gesprekken dat bewustzijn over de mogelijke gevaren, invloed heeft op de manier van communiceren en het gebruik van informatiebeveiligingstechnologie. De conclusies uit dit onderzoek zijn toepasbaar op onderzoeksjournalisten die ervaring hebben met thema's als nationale veiligheid, politie, justitie, inlichtingendiensten en (georganiseerde) criminaliteit. In hoeverre de bevindingen ook opgaan voor de Nederlandse journalistiek in het algemeen, zal toekomstig onderzoek moeten uitwijzen.

Voorwoord

Voor u ligt mijn scriptie ter afronding van de master Journalistiek en Nieuwe Media aan de Universiteit van Leiden. Een onderzoek naar de ervaringen van Nederlandse onderzoeksjournalisten met overheidssurveillance en de impact daarvan op de journalistieke bescherming van vertrouwelijke bronnen. Deze scriptie is het resultaat van een half jaar hard werken, een proces dat nooit volbracht had kunnen worden zonder de hulp van anderen.

Veel dank ben ik verschuldigd aan mijn begeleider Alexander Pleijter, voor het beantwoorden van talloze mailtjes, zijn hulp bij het zoeken naar geschikte respondenten en de vrijheid die hij mij gaf in het vormgeven van mijn onderzoek. Dank ook aan mijn studiegenoten voor hun waardevolle inzichten tijdens de scriptiebijeenkomsten en daarbuiten. Daarnaast wil ik mijn waardering uitspreken voor mijn lieve familie en vrienden, die mij gedurende het gehele proces hebben aangemoedigd en gesteund door naar mijn verhalen te luisteren en mijn scriptie van begin tot eind te lezen. Mijn dank is groot.

Tot slot wil ik mijn dankbaarheid uiten aan alle respondenten uit het onderzoek, die ondanks hun overvolle agenda's bereid waren mij te woord te staan. Het was een feest om met hen te praten en te luisteren naar hun inspirerende verhalen. Zonder hen was deze scriptie niet mogelijk geweest. Nogmaals dank!

Veel leesplezier!

Nikki IJzerman

Den Haag, 1 augustus 2023

Inhoudsopgave

1. Inleiding

Vanaf het moment dat Stella Braam haar loopbaan als onderzoeksjournalist begon, werd ze door de inlichtingendiensten in de gaten gehouden. Dat bleek uit onderzoek van NRC-journalist Joep Dohmen, die daarover in augustus 2022 een artikel schreef. Het dossier dat de AIVD over haar bijhield, telt ruim driehonderd pagina's. Een product van ruim 35 jaar spionage. In de zomer van 2022 kreeg Braam de documenten in te zien, hoewel grote stukken onleesbaar waren gemaakt. De pagina's die ze wel kon lezen, gingen over haar werk als onderzoeksjournalist én haar persoonlijke leven. Het zorgde voor angst en boosheid bij Braam, die weet dat ze niet de enige is (Dohmen, 2022a).

De Nederlandse inlichtingendiensten hebben altijd al nauwe banden gehad met de journalistiek. Soms worden journalisten ongewenst gevolgd, zoals in het geval van Braam, terwijl anderen juist actief samenwerken met de AIVD of MIVD. Uit onderzoek van *NRC* bleek dat inlichtingendiensten systematisch journalisten werven als bron, informant of spion (Dohmen, 2022b). Dat lang niet alle journalisten toehappen, maakt het niet minder gevaarlijk. Wie alleen al wordt verdacht van spionage voor Westerse veiligheidsdiensten loopt enorme risico's, met name in landen als Rusland, China of Iran (Dohmen, 2022b).

De ronsel- en afluisterpraktijken van inlichtingendiensten brengen niet alleen journalisten maar ook hun bronnen in gevaar. Braam voelt zich onzeker sinds ze weet dat de AIVD haar in de gaten houdt, zo vertelt ze in gesprek met *NRC*. "Ik moet mijn bronnen kunnen beschermen. Maar zonder de wetenschap dat de AIVD gestopt is, kan ik dat niet" (Dohmen, 2022a). De woorden van Braam zijn opmerkelijk, omdat de overheid de laatste jaren juist stappen heeft ondernomen om die onzekerheid tegen te gaan. Zo werd in 2016 de Wet op de inlichtingen- en veiligheidsdiensten (Wiv) gewijzigd nadat twee journalisten van *De Telegraaf* een rechtszaak hadden aangespannen tegen de Nederlandse staat. De AIVD zou bijzondere bevoegdheden hebben ingezet om de bronnen van deze journalisten te achterhalen en daarmee het Europees Verdrag voor de Rechten van de Mens hebben geschonden (*Kamerstukken II*, 2016/17, 34588, nr. 3, p. 48). De wetswijziging zou het inlichtingendiensten lastiger maken om dergelijke bevoegdheden in de toekomst te gebruiken en daarmee journalisten en hun bronnen beter beschermen.

Onderzoeksjournalisten beroepen zich regelmatig op anonieme bronnen. Het zijn mensen die betrouwbare informatie openbaar maken en daarmee hun vrijheid of zelfs veiligheid op het spel zetten. Het is de ethische verantwoordelijkheid van journalisten om voorzichtig met

die informatie om te gaan. “De journalist beschermt bronnen aan wie hij vertrouwelijkheid heeft toegezegd,” zo luidt een van de regels uit de journalistieke code van het Nederlands Genootschap van Hoofdredacteuren (2008). Omdat het hier gaat om een code en niet om een recht, kunnen journalisten na uitspraak van een rechter alsnog gedwongen worden hun bronnen te onthullen. Dit gebeurt alleen in uitzonderlijke situaties, bijvoorbeeld als de staatsveiligheid in gevaar is (Evers, 2011, p. 11). Maar zoals Stella Braam al bewees, gaan overheden lang niet altijd volgens deze officiële gerechtelijke kanalen te werk.

Dat niet alleen journalisten maar praktisch iedereen doelwit kan worden van overheidsspionage, kwam in 2013 pijnlijk naar buiten. Klokkenluider Edward Snowden onthulde dat jaar hoe Amerikaanse inlichtingendiensten jarenlang illegaal het telefoon- en mailverkeer van burgers verzamelden. De enorme omvang van deze overheidssurveillance was wereldwijd groot nieuws. In de wetenschappelijke wereld, en specifiek binnen het vakgebied van de journalistieke studies, werden de onthullingen van Snowden aangegrepen voor nieuw onderzoek naar de aard, omvang en gevolgen van digitale overheidsspionage voor de journalistieke praktijk (Bradshaw, 2017, p. 335).

Uit een eerste verkenning van deze literatuur valt één concept direct op: het zogenoemde *chilling effect*. Het gevoel constant in de gaten te worden gehouden, werkt verlammend. Voor journalisten, die bang zijn de anonimiteit van hun bronnen niet langer te kunnen waarborgen en om die reden hun onderzoek staken. En voor bronnen, die minder snel bereid zijn gevoelige informatie te delen met journalisten uit angst dat hun identiteit op straat komt te liggen. Dit heeft niet alleen ingrijpende gevolgen voor de journalistiek, maar voor de maatschappij als geheel. Als journalisten niet in staat zijn het publiek te informeren over misstanden, kunnen zij onmogelijk hun rol als waakhond van de samenleving vervullen (Bradshaw, 2017, p. 336).

Vanzelfsprekend zijn er voor journalisten mogelijkheden om zich te beschermen tegen hackers en digitale spionage. Huib Modderkolk, onderzoeksjournalist van *De Volkskrant* die voor zijn boek *Het is oorlog maar niemand die het ziet* in de wereld van inlichtingen- en veiligheidsdiensten dook, beschrijft hoe hij verschillende technieken gebruikte om zo onopvallend mogelijk te werk te gaan. Hij schafte prepaidtelefoons aan, wisselde regelmatig van simkaart, kocht nieuwe, opgeschoonde computers die alleen in noodgevallen met het internet verbonden waren en gebruikte versleutelde chatprogramma’s om mailverkeer met collega’s en bronnen te onderhouden (Modderkolk, 2022, pp. 27–28). Allemaal voorzorgsmaatregelen om te voorkomen dat gevoelige informatie in handen zou vallen van de verkeerde mensen.

Behalve Modderkolk hebben ook andere Nederlandse onderzoeksjournalisten zich

verdiept in de digitale wereld en de gevaren die erachter schuilgaan. Daniël Verlaan schreef in zijn boek *Ik weet je wachtwoord* over hackers en online criminaliteit. Volgens hem hebben mensen nauwelijks door hoe kwetsbaar ze zijn en dat maakt dat vrijwel iedereen ten prooi kan vallen aan internetcriminelen (Verlaan, 2020). Ook Maurits Martijn en Dimitri Tokmetzis hoopten met hun boek *Je hebt wél iets te verbergen* de bewustwording over de gevaren van het internet te vergroten. Zij schreven hoe online overheidssurveillance en datamining door grote techbedrijven de privacy van burgers ernstig in gevaar brengen en ingrijpende gevolgen kan hebben voor het functioneren van een democratie (Martijn & Tokmetzis, 2016).

Als burgers en journalisten op de hoogte zijn van de gevaren achter het internet, dan kunnen ze maatregelen nemen om zichzelf beter te beschermen. In het post-Snowden tijdperk ondernemen ook steeds meer nieuwsmedia actie om hun informatie te beveiligen. De technologieën, tools en software die zij hiervoor kunnen gebruiken, zijn door verschillende onderzoekers al verkend (Bradshaw, 2017; Di Salvo, 2021; McGregor, 2014). Uit dergelijk onderzoek blijkt echter dat er nog steeds journalisten zijn die de veiligheidsrisico's (al dan niet terecht) onderschatten of onvoldoende op de hoogte zijn van de beschikbare informatiebeveiligings-technologie (Crete-Nishihata et al., 2020; Henrichsen, 2020; Kunert et al., 2022). In hoeverre dit ook voor Nederlandse journalisten geldt, is een vraag die na dit onderzoek hopelijk kan worden beantwoordt.

Onderzoek dat in de afgelopen tien jaar is verschenen, is hoofdzakelijk gericht op ofwel Amerikaanse journalistiek ofwel Engelstalige nieuwsmedia (Lashmar, 2017; Waters, 2018). Het doel van deze scriptie is om de bevindingen uit de internationale wetenschappelijke literatuur, zoals samengevat in hoofdstuk 2, toe te passen op de Nederlandse context. De focus ligt op onderzoeksjournalisten vanuit de redenering dat zij, in vergelijking tot 'gewone' journalisten, vaker onderzoek doen naar gevoelige onderwerpen en om die reden meer werkervaring hebben met anonieme bronnen. De onderzoeksvraag die daarbij hoort, luidt als volgt:

> **Hoe ervaren Nederlandse onderzoeksjournalisten de mogelijke dreiging van digitale overheidssurveillance en hoe beïnvloedt dit hun werkwijze wat betreft de bescherming van vertrouwelijke bronnen?**

Om de hierboven gestelde onderzoeksvraag te beantwoorden, zijn interviews gehouden met Nederlandse onderzoeksjournalisten die mogelijk groter risico lopen op overheidssurveillance, omdat zij werken aan gevoelige thema's zoals politie, justitie en inlichtingendiensten. In hoeverre ervaren zij een *chilling effect*? Hoe beïnvloedt dit hun werkwijze met vertrouwelijke

bronnen? Welke vormen van informatiebeveiliging passen ze toe in hun werk en hoe heeft dit hun omgang met bronnen veranderd? In hoofdstuk 3 zal deze methode in meer detail worden toegelicht. Hoofdstuk 4 bevat de resultaten van de interviews, evenals de antwoorden op de deelvragen. De hoofdvraag wordt beantwoord in de conclusie (hoofdstuk 5).

2. Theoretisch kader

In deze studie wordt onderzocht hoe de dreiging van overheidssurveillance door Nederlandse onderzoeksjournalisten wordt ervaren en hoe zij hierop anticiperen wanneer ze werken met vertrouwelijke bronnen. Het is aannemelijk dat er sprake kan zijn van een *chilling effect*, zowel bij journalisten als bronnen. Paragraaf 2.1 van dit theoretische kader gaat over de relatie tussen bronnen en journalisten in het algemeen, met speciale aandacht voor vertrouwelijke bronnen. In 2.2 wordt het *chilling effect* uitgelicht, waarin de definitie, oorsprong en ontwikkeling van het concept worden besproken. Paragraaf 2.3 gaat over informatiebeveiliging en is vormgegeven rondom de vraag welke strategieën journalisten gebruiken om vertrouwelijke informatie, zoals de identiteit van anonieme bronnen, te beschermen. Tot slot wordt in 2.4 gekeken naar onderzoek dat vergelijkbaar is met deze scriptie en waarin de thema's bronbescherming, surveillance en informatiebeveiliging samenkomen.

2.1. Journalisten en hun bronnen

Of het nu gesproken of geschreven bronnen zijn, ooggetuigenverslagen of duiding door experts, officiële beleidsdocumenten of tweets van politici: bronnen zijn essentieel voor het werk van journalisten. In deze paragraaf wordt gekeken naar het belang van journalistiek brongebruik, de relatie tussen bronnen en journalisten en de omgang met anonieme bronnen.

2.1.1. Brongebruik als journalistieke norm

Het belang van brongebruik is onderdeel van een bredere professionele journalistieke standaard die zich halverwege de twintigste eeuw in westerse landen begon te ontwikkelen. Onderdeel van deze professionalisering was het verschijnen van ethische codes, die journalisten hielpen hun positie als waakhonden van de samenleving te legitimeren (Deuze, 2005, p. 449). Inmiddels hebben ook de meeste Nederlandse nieuwsmedia een eigen journalistieke code online staan. Hoewel deze codes niet helemaal identiek zijn aan elkaar, bevatten ze over het algemeen dezelfde journalistieke normen en waarden. Deze zijn door Mark Deuze (2005, p. 447) samengevat in vijf categorieën: (1) publieke dienstverlening, (2) objectiviteit, (3) autonomie, (4) urgentie en (5) ethiek.

Gekeken naar deze categorisering, zijn bronnen vooral belangrijk voor het waarborgen van de journalistieke objectiviteit. Hoewel het objectiviteitsideaal ter discussie staat – niemand is immers volledig objectief – dienen journalisten dit altijd na te streven (Deuze, 2005, p. 448).

Zo wordt verwacht dat zij in hun verslaggeving persoonlijke voorkeuren en opvattingen buiten beschouwing laten en in plaats daarvan gebruik maken van het attributieprincipe: informatie wordt direct gelinkt aan bronnen, bijvoorbeeld met quotes. Het voordeel hiervan is dat journalisten in staat zijn inhoudelijk kritische uitspraken te doen, terwijl ze de verantwoordelijkheid ervan bij hun bronnen leggen. Zo lang journalisten verschillende perspectieven aan bod laten komen, kunnen ze tot op zekere hoogte toezien op evenwichtige, neutrale en eerlijke berichtgeving (Carlson, 2009, pp. 527–528).

Ook voor het verifiëren van feiten – een andere belangrijke journalistieke norm – zijn bronnen belangrijk. Over het algemeen geldt dat journalisten hun informatie aan ten minste één bron dienen voor te leggen. De gevoeligheid van informatie, beschikbaarheid van andere bronnen en betrouwbaarheid van de originele bron kunnen redenen zijn voor een journalist om informatie te dubbelchecken. 'Eén bron is geen bron' is niet voor niets een veelgehoord journalistiek credo. Overigens is bronvermelding niet alleen een belangrijke professionele norm. Het stelt nieuwsconsumenten in staat zelfstandig informatie te verifiëren, wat het werk van journalisten transparanter maakt. Zoals verderop in deze paragraaf zal blijken, is het gebruik van anonieme bronnen in die zin problematisch, omdat die niet te verifiëren zijn en daarmee de geloofwaardigheid van journalisten wordt ondermijnd (Shapiro et al., 2013, p. 666).

2.1.2. De dans tussen journalisten en hun bronnen

Journalisten proberen in hun verslaggeving zo dicht mogelijk bij de waarheid te komen, een proces waarbij ze dus sterk afhankelijk zijn van bronnen. Maar bronnen worden vaak gedreven door een persoonlijk belang en zijn daarom – net als journalisten zelf – nooit helemaal objectief. De relatie tussen journalisten en hun bronnen is er dan ook een van zorgvuldige onderhandeling, aangezien beide partijen zich blootstellen aan risico's. Enerzijds wil de journalist zijn geloofwaardigheid behouden, anderzijds zetten bronnen hun carrière op het spel door in de media te verschijnen (Berkowitz, 2009, p. 103). Niet voor niets wordt die relatie in de wetenschappelijke literatuur vaak metaforisch beschreven als een dans of tango (Carlson, 2009; Reich, 2006; Van Aelst & Vliegenthart, 2014).

De tango-metafoor werd in 1979 door socioloog Herbert Gans bedacht en impliceert een zekere machtsstrijd tussen journalisten en bronnen. Want wie leidt eigenlijk de dans? Uit onderzoek van Reich (2006), waarvoor hij reconstructie-interviews hield met Israëlische verslaggevers, bleek dat bronnen in de nieuws-ontdekkingsfase vaak het initiatief hebben. Informatie voor een potentieel nieuwsverhaal komt dan meestal van woordvoerders van officiële publieke instituties, zoals het leger, de politie of overheidsinstanties. Later, in de

nieuws-verzamelingsfase, verschuift het initiatief. Dan zijn het de journalisten die de boventoon voeren en naar aanleiding van extra informatie opnieuw contact zoeken met bronnen.

Van Aelst en Vliegenthart (2013) onderzochten het Nederlandse medialandschap en schetsen een ander beeld van de journalist-bron-relatie. De auteurs onderzochten de relatie tussen politieke verslaggeving en Kamervragen en concludeerden dat de invloed van de media op de politiek over het algemeen groter is dan andersom. Media zijn in staat politici te inspireren tot het stellen van Kamervragen, terwijl politici zelf weinig invloed hebben op de agenda van nieuwsmedia. Dat wil niet zeggen dat ze totaal geen macht hebben. Kamerleden spelen vaak in op maatschappelijke problemen en hopen met de media-aandacht die ze daarvoor generen, het publieke debat te beïnvloeden. Toch zijn het de journalisten die bepalen wie wél en wie geen stem krijgen in de media, waarmee ze nog steeds een belangrijke rol vervullen als poortwachters tussen de politicus en zijn kiezer (Van Aelst & Vliegenthart, 2014, pp. 404–405).

2.1.3. Het dilemma van anoniem brongebruik

Eerder deze paragraaf werd duidelijk dat bronvermelding essentieel is voor het verifiëren van journalistiek werk. Toch komt het wel eens voor dat bronnen anoniem willen blijven, bijvoorbeeld omdat ze vertrouwelijke of anderszins gevoelige informatie openbaar maken. Als journalisten hiermee instemmen, zijn zij verplicht de identiteit van hun bronnen te beschermen. Hoewel dit ingaat tegen het attributieprincipe, stelt het journalisten in staat verhalen te vertellen die anders misschien niet naar buiten zouden komen. Met andere woorden, media kunnen hun maatschappelijke waakhondfunctie nog beter vervullen als zij zich in uitzonderlijke situaties mogen beroepen op anonieme bronnen (Vobič & Kovačič, 2015, pp. 591–593).

Onderzoek van Matt Duffy (2014, pp. 244-245) laat zien dat het gebruik van anonieme bronnen nooit onomstreden is geweest. De auteur analyseerde Amerikaanse ethische codes en journalistieke tekstboeken uit de periode 1907-2007 en zag dat in de eerste helft van de twintigste eeuw in geen van de boeken werd gerept over anonieme bronnen. Hoewel anoniem brongebruik in die periode wel voorkwam, was deze journalistieke werkwijze nog niet echt geaccepteerd als professionele norm. Dit veranderde vanaf de jaren zeventig, toen onder meer met de onthulling van het Watergateschandaal de meerwaarde van anonieme bronnen werd bevestigd. In steeds meer journalistieke codes werd het belang van anoniem brongebruik erkend, mits de journalist voldoende kon onderbouwen dat het openbaar maken van de identiteit van zijn bron schadelijk zou kunnen zijn en dat de informatie op geen enkele andere manier kon worden verkregen (Duffy, 2014, pp. 248–249).

Toch is anoniem brongebruik nog steeds uitzondering op de regel. Dat is niet voor niets.

In de decennia rond de eeuwwisseling werd de journalistieke wereld opgeschrikt door een aantal schandalen. Zo kwam de Amerikaanse pers flink onder vuur te liggen vanwege zijn sterke afhankelijkheid van anonieme bronnen in de verslaggeving van de Lewinsky-affaire, met name uit het kamp van president Clinton. Een aantal jaar later raakte de *New York Times* in opspraak toen bleek dat één van hun verslaggevers jarenlang informatie en quotes gefabriceerd had, waarbij hij zich baseerde op zogenaamd anonieme bronnen (Duffy, 2014, p. 252). Nieuwsmedia zagen in dat er strengere richtlijnen moesten komen voor het gebruik van anonieme bronnen. Deze werden opgenomen in de nieuwe codeboeken. Een inhoudsanalyse van krantenartikelen uit 2003 en 2004 liet tevens zien dat het gebruik van anonieme bronnen in Amerikaanse dagbladen aanzienlijk was afgenomen (Martin-Kratzer & Thorson, 2007).

Als gevolg van de verschillende schandalen werd het debat rondom anonieme bronnen nieuw leven in geblazen. Academici zijn bijvoorbeeld verdeeld over de vraag of anoniem brongebruik de geloofwaardigheid van journalisten ondermijnt. Sternadori en Thorson (2009) constateerden op basis van interviews dat het gebruik van anonieme bronnen de perceptie van lezers op de geloofwaardigheid van een nieuwsverhaal negatief beïnvloedde, zelfs als het ging om prijswinnend journalistiek onderzoek. Smith (2007) daarentegen, vond geen overtuigend bewijs voor een negatief verband tussen anoniem brongebruik en journalistieke geloofwaardigheid. Respondenten uit zijn onderzoek beoordeelden verhalen mét anonieme bronnen nagenoeg even geloofwaardig als verhalen zonder anonieme bronnen.

Behalve de kwestie rondom geloofwaardigheid, vragen academici zich ook af in hoeverre anoniem brongebruik ethisch verantwoord is. Om die vraag te beantwoorden, grijpen Duffy en Freeman (2011, p. 310) terug op de theorie van het utilitarisme: de morele waarde van een handeling wordt bepaald door de hoeveelheid geluk dat het produceert. Volgens de auteurs is anoniem brongebruik dan ook alleen gerechtvaardigd als de voordelen opwegen tegen de nadelen. Het is niet de bedoeling dat bronnen hun anonimiteit misbruiken om lasterlijke uitspraken te doen over een andere partij, omdat ze hier niet aansprakelijk voor kunnen worden gehouden. Anderzijds biedt anonimiteit uitkomst voor bronnen die met hun onthullingen groot persoonlijk risico lopen, zoals klokkenluiders. Het is aan journalisten om hierin een keuze te maken en het belang van een verhaal af te wegen tegen hun eigen geloofwaardigheid.

2.2. Definitie, oorsprong en theoretische ontwikkeling van het *chilling effect*

Deze paragraaf gaat over het *chilling effect*, een theorie die wordt gebruikt om te beschrijven hoe censuur kan leiden tot angst en onzekerheid bij schrijvers en journalisten, met als gevolg

dat zij afzien van hun recht op vrijheid van meningsuiting. Die censuur kan op allerlei manieren voorkomen: heel concreet in de vorm van een publicatieverbod of subtieler als gevolg van ambigue wetgeving of, om bij het onderwerp van deze scriptie te blijven, (online) spionage en surveillance. Dit stelt journalisten die werken met gevoelige informatie voor een moeilijk vraagstuk: zijn zij nog in staat de identiteit van vertrouwelijke bronnen te beschermen? Bij twijfel kan een *chilling effect* optreden: journalisten besluiten hun onderzoek bijvoorbeeld te staken. Steeds vaker duikt de term op binnen mediastudies, hoewel het zijn wortels heeft in het Angelsaksische recht (Townend, 2017, pp. 73–73). Hoe het *chilling effect* zich heeft ontwikkeld tot een begrip met een breed theoretisch fundament, wordt in deze paragraaf besproken.

2.2.1. De juridische oorsprong van het chilling effect

Rechtsgeleerde Frederick Schauer gaf in 1978 als eerste een theoretische basis aan het *chilling effect*. In essentie, zo schreef hij, gaat het om een afschrikeffect (*deterrence theory*): bepaald gedrag wordt ontmoedigd omdat er een straf of sanctie op staat. Een boete voor het overtreden van de snelheidslimiet moet voorkomen dat mensen te hard rijden, net zoals het risico op een gevangenisstraf voor zware mishandeling moet voorkomen dat mensen met elkaar op de vuist gaan. In deze voorbeelden is een *chilling effec*t wenselijk: het voorkomt dat mensen strafbare feiten plegen, juist omdát ze strafbaar zijn (Schauer, 1978, p. 689). Dit is echter niet hoe het *chilling effect* voor het eerst werd gebruikt.

Een kwart eeuw voordat Schauer zijn theorie op papier zette, werd in een Amerikaanse rechtszaak voor het eerst gerefereerd aan het *chilling effect*. Om de verspreiding van communistisch gedachtegoed te onderdrukken, waren werknemers van de staat Washington verplicht een loyaliteitsede af te leggen, waarin ze trouw zwoeren aan de regering van de Verenigde Staten en moesten bevestigen geen lid te zijn van een communistische groepering. Het Amerikaanse Hof zag dat burgers werden afgeschrikt om gebruik te maken van hun recht op vrijheid van meningsuiting, omdat onduidelijk was wat wel en wat niet was toegestaan onder deze ede. Ook ‘gewetensvolle’ burgers hadden last van een *chilling effect*, simpelweg omdat niemand precies wist wanneer ze strafbaar waren. De loyaliteitsede, zo oordeelde een rechter in 1952, was in strijd met het Eerste Amendement van de Amerikaanse grondwet en werd om die reden afgeschaft (Penney, 2021, p. 1468).

In een ideale wereld veroordeelt het rechtssysteem alleen mensen die de wet overtreden. Burgers die zich netjes aan de regels houden, hoeven dus niet bang te zijn voor straf. Maar de rechterlijke macht bestaat uit mensen en waar mensen werken, worden fouten gemaakt. Vage of te brede wetgeving, misinterpretatie door rechters of vooroordelen van juryleden: het zijn

voorbeelden die laten zien dat de rechtspraak onzeker en feilbaar is. De mogelijkheid dat legitiem gedrag toch bestraft kan worden als gevolg van fouten in het rechtssysteem, werkt beangstigend (Schauer, 1978, pp. 694–696). Schauer schreef daarom in 1978: "A chilling effect occurs when individuals seeking to engage in activity protected by the first amendment are deterred from so doing by governmental regulation not specifically directed at that protected activity" (Schauer, 1978, p. 693).

Hoewel bovenstaande definitie van het *chilling effect* nog steeds invloedrijk is binnen de wetenschappelijke wereld, is er ook kritiek. Volgens Jonathon Penney is er weinig empirisch bewijs dat *deterrence theory* in praktijk ook werkt. Mensen maken geen rationele kosten-batenanalyse voordat ze een beslissing nemen, zo schrijft hij, en ze zijn al helemaal niet actief bezig met wat de wet hen wel of niet voorschrijft. Bovendien is Schauers' definitie van het *chilling effect* té beperkt en niet toepasbaar buiten de juridische context. Penney pleit daarom voor een herdefiniëring, zodat de theorie ook in andere situaties kan worden gebruikt. Bijvoorbeeld in het geval van (online) surveillance (Penney, 2021, pp. 1470–1472).

2.2.2. Surveillance, dataveillance en online gedrag

De Amerikaanse privacy-expert Daniel Solove deed in 2006 al wat Jonathon Penney in zijn artikel betoogde: hij haalde het *chilling effect* uit zijn juridische context en gaf een nieuwe dimensie aan de theorie. Hij schreef hoe sociale controle in de vorm van overheidssurveillance kan leiden tot zelfcensuur en remmingen in menselijk gedrag. Dit is op zichzelf niet per se schadelijk. Mensen zijn bereid om een deel van hun privacy op te geven als dit hun veiligheid vergroot. Camera's in openbare ruimtes bijvoorbeeld, ontmoedigen criminelen om delicten te plegen, omdat de kans groter is dat ze worden gepakt. Dus is de samenleving als geheel beter af mét dan zonder dat toezicht.

Te veel sociale controle heeft echter ook een keerzijde. Het beperkt mensen in hun vrijheid, creativiteit en zelfontwikkeling, omdat zij het gevoel hebben zich te moeten gedragen naar dat wat aanvaardbaar wordt gevonden. In situaties waar mensen zich bewust zijn van de mogelijkheid van surveillance, maar nooit precies weten wanneer ze worden bespied, is de kans op een *chilling effect* extra groot (Solove, 2006, pp. 493–495).

Wat geldt voor de fysieke wereld, geldt ook voor de digitale wereld. Online surveillance en de continue digitale dataverzamelingspraktijken van overheden en bedrijven – door Büchi et al. (2022, p. 1) gedefinieerd als *dataveillance* – beïnvloeden online gedrag. Naarmate mensen zich meer en meer bewust worden van de aanwezigheid van *dataveillance*, verandert ook hun houding ten aanzien van digitale communicatie. Ze zien er vanaf uit angst voor het achterlaten

van een digitaal spoor en zijn voorzichtiger in hun online gedrag door geen persoonlijke meningen te delen of bepaalde onderwerpen te vermijden (Büchi et al., 2022, pp. 8–9).

Wat Büchi et al. (2022) beschrijven, is een *chilling effect* dat kan optreden wanneer surveillance en dataveillance de privacy van mensen schenden. Maar volgens sommige experts werkt de praktijk heel anders. Mensen zijn niet minder gaan internetten sinds ze weten van de spionagepraktijken van overheden. Het is een fenomeen dat ook wel de privacy-paradox wordt genoemd; mensen zeggen wel dat ze privacy belangrijk vinden, maar handelen hier nauwelijks naar (Solove, 2021, p. 2). Dat komt omdat veel mensen het als zinloos ervaren: het is onmogelijk om je eigen privacy volledig onder controle hebben. Mensen berusten in het feit dat ze waarschijnlijk nooit genoeg kennis zullen hebben over manier waarop hun persoonlijke data worden verzameld, opgeslagen en geanalyseerd, waardoor ze geen serieuze maatregelen nemen om die gegevens te beschermen (Solove, 2021, p. 5). Hoewel niet iedereen gelooft in de privacy-paradox – een debat waarover in deze studie verder niet zal worden uitgeweid – laat het goed zien dat het *chilling effect* zelf ook geen waterdichte theorie is, maar altijd op een kritische manier moet worden bekeken.

2.2.3. Journalistiek onderzoek in het surveillancetijdperk

Hoewel in theorie iedereen doelwit kan zijn van digitale overheidssurveillance, is het risico voor journalisten extra groot. Zij zijn niet alleen verantwoordelijk voor hun eigen veiligheid, maar ook voor die van hun bronnen. De dreiging van surveillance kan dan ook aan beide kanten leiden tot een *chilling effect*. Bij journalisten die het gevoel hebben niet te kunnen instaan voor de veiligheid van hun bronnen en bijvoorbeeld kiezen om niet te publiceren. En bij bronnen die maatschappelijke problemen niet meer bespreekbaar durven te maken uit angst dat hun identiteit op straat komt te liggen, met alle gevolgen van dien (Bradshaw, 2017, p. 336).

Naar aanleiding van de onthullingen van Edward Snowden in 2013 deed PEN American Center – een non-profitorganisatie die opkomt voor vrijheid van meningsuiting door de bevordering van literatuur en mensenrechten – grootschalig enquête-onderzoek naar de impact van massasurveillance op schrijvers wereldwijd. Vrijheid van meningsuiting is immers een belangrijke voorwaarde om dit beroep te kunnen uitoefenen, zo redeneerden de auteurs. Dat de spionagepraktijken van overheden die voorwaarde ernstig onder druk zetten, blijkt wel uit de onderzoeksresultaten. Een aanzienlijk percentage van de in totaal 772 respondenten gaf aan zichzelf te censureren uit angst voor overheidssurveillance. Dit betekende wegblijven van onderwerpen die controversieel zouden kunnen zijn, vermijden van sociale media en waakzaamheid bij alle andere vormen van digitale communicatie (PEN American Center, 2015,

pp. 9–11).

PEN's International Survey of Writers is vergelijkbaar met het rapport van Pew Research Center (2015), maar verschilt in het feit dat laatstgenoemde onderzoek zich specifiek richtte op (Amerikaanse) onderzoeksjournalisten. Hieruit bleek dat de meeste onderzoeksjournalisten (64%) vermoeden dat de Amerikaanse overheid gegevens over hun communicatie verzamelt. Hoewel dit weinig journalisten tegenhield om een bron of verhaal na te streven, gaf 49% van de respondenten wel toe een verandering te hebben doorgevoerd in de manier waarop ze gevoelige documenten opslaan of delen, terwijl 29% aangaf ook hun communicatie met collega's te hebben aangepast (Pew Research Center, 2015, pp. 2–3). Van een verlammende angst kan desalniettemin nog niet worden gesproken. Dit is anders voor journalisten die werken aan gevoelige onderwerpen als nationale veiligheid, terrorisme, surveillance, inlichtingendiensten en georganiseerde misdaad. Onder deze groep is de angst voor een *chilling effect* een stuk groter (Mills, 2019, p. 704).

Dat journalisten van over de hele wereld steeds vaker een *chilling effect* ervaren, wordt door onderzoek van UNESCO ondersteund (Posetti, 2017, p. 106). Omdat de kosten voor het digitaal beveiligen van informatie of het juridisch bestrijden van inbeslagname door autoriteiten vaak heel hoog zijn, zoeken journalisten naar alternatieve oplossingen. Dit uit zich onder andere in het verwijderen van archiefmateriaal. Maar niet alleen journalisten zelf zijn voorzichtiger. Ook bronnen zijn terughoudender in hun samenwerking met journalisten wanneer dreiging van overheidssurveillance aannemelijk is. Vooral vertrouwelijke bronnen zijn daardoor minder snel bereid om gevoelige informatie te delen. En dat heeft weer invloed op de werkwijze van journalisten:

> "To really discuss with people we prefer to avoid electronic means or social networks. The Snowden Affair turned upside down the work of journalists... It's harder to speak to people. We really have to go out and meet them. It's face to face" (Posetti, 2017, p. 105).

2.3. Informatiebeveiliging voor onderzoeksjournalisten

Wetenschappelijk onderzoek laat zien dat journalisten zich steeds meer bewust zijn van de mogelijke dreiging van overheidssurveillance. Dat zij om die reden geneigd zijn hun gedrag en werkwijze aan te passen, is problematisch, omdat het de waakhondfunctie van de journalistiek in gevaar brengt. Desalniettemin zijn er voor journalisten (en burgers in het algemeen) mogelijkheden om gevoelige informatie goed te beschermen. Die informatiebeveiligings-

strategieën worden in deze paragraaf besproken, evenals de perceptie van journalisten hierop. Want hoe groot het gevaar in theorie ook mag zijn, in de praktijk blijkt ook dat door onwetendheid, onmacht en onderschatting veel journalisten zich nog onvoldoende tegen deze gevaren beschermen.

2.3.1. Informatiebeveiligingstechnologie voor bronnen

In een wereld die meer en meer digitaal wordt, verloopt journalistiek onderzoek en communicatie met bronnen ook steeds vaker online. Dit maakt journalisten kwetsbaar voor hackers en digitale spionnen. In de vorige paragraaf werd duidelijk dat zij de risico's verkleinen door onder andere terug te grijpen op analoge vormen van communicatie. Vanaf 2013 zijn er echter allerlei nieuwe softwareplatforms opgericht die middels een versleutelde verbinding vertrouwelijke communicatie tussen journalisten en bronnen faciliteren. *SecureDrop* is een voorbeeld van zo'n platform en, zo bleek uit onderzoek van Di Salvo (2021), wordt inmiddels door tientallen overwegend Amerikaanse en Westerse nieuwsorganisaties gebruikt.

De Nederlandse evenknie van SecureDrop is *Publeaks*, een klokkenluidersplatform dat samenwerkingen onderhoudt met meer dan veertig Nederlandse nieuwsorganisaties. Het is een stichting die klokkenluiders op een veilige manier in contact wil brengen met media. *Publeaks* kan het beste gezien worden als een technische tool: een gespecialiseerd team verzorgt de technologische infrastructuur, maar heeft verder geen enkel aandeel in de eventuele publicatie van nieuwsartikelen. Dat betekent ook dat journalisten nog altijd zelf de gelekte informatie dienen te verifiëren (Porlezza & Di Salvo, 2020).

2.3.2. Waarom journalisten nauwelijks informatiebeveiligingstechnologie gebruiken

Journalisten kunnen zich op allerlei manieren beschermen tegen digitale pottenkijkers. Toch zijn er maar weinig die dit echt goed doen. Henrichsen (2020, p. 333) interviewde Amerikaanse journalisten, ontwikkelaars en beveiligingsexperts over de percepties van journalisten op informatiebeveiligingstechnologie en onderscheidde vijf obstakelpunten die journalisten ervan weerhouden om dergelijke tools in hun dagelijks werk te gebruiken: (1) onderschatting van de veiligheidsrisico's; (2) het ontbreken van begrip voor beveiligingstechnologie in de redactiecultuur; (3) de (onterechte) overtuiging dat informatiebeveiliging alleen nodig is voor journalisten die werken met overheidsbronnen; (4) het ontbreken van kennis over informatiebeveiligingstechnologie bij bronnen; en (5) onzekerheid over de effectiviteit van informatiebeveiligingstechnologie.

Onderzoek dat vergelijkbaar is met dat van Henrichsen (2020) leverde dezelfde

resultaten op. Kunert et al. (2022) toonden aan dat journalisten overal ter wereld tegen dezelfde barrières aanlopen als hun Amerikaanse collega's. Met name het gebrek aan kennis en vaardigheden op het gebied van digitale informatiebeveiliging is voor veel journalisten een groot probleem. Hoewel een enkeling geen beveiligingstools nodig denkt te hebben – de onderwerpen waaraan ze werken zijn van weinig belang voor anderen – zien de meeste journalisten de waarde van digitale bronbescherming wel in. Ze weten alleen niet hoe. Niet voor niets zijn het vaak de journalisten met bovengemiddelde technische vaardigheden die massasurveillance als het meest bedreigend ervaren (Waters, 2018, p. 1302).

Journalisten bij wie het ontbreekt aan technische skills passen hun werkwijze op andere manieren aan. Ze onderhouden het contact met bronnen bijvoorbeeld liever face-to-face of blijven helemaal weg van digitale communicatie (Kunert et al., 2022, p. 771; Posetti, 2017, p. 108). Sommigen gebruiken versleuteld e-mailverkeer en vermijden cloudopslag. Maar zwaarder geschut – zoals het installeren van de Tor Browser, een webbrowser die internetactiviteit volledig anonimiseert – wordt door veel journalisten toch vooral als een belemmering ervaren (Waters, 2018, p. 1310).

De ondervraagde regiojournalisten uit het onderzoek van Bradshaw (2017, p. 344) schoven de verantwoordelijkheid voor informatiebeveiliging geregeld af naar hun bronnen, vanuit de redenering dat zij vaak zelf al op hun hoede zijn voor de mogelijke risico's. Tegelijkertijd spelen ook andere factoren een rol. Sommige journalisten twijfelen of ze hun bronnen moeten laten werken met strenge beveiligingsapparatuur. Het kan hen afschrikken, omdat ze constant herinnerd worden aan het feit dat ze vertrouwelijke informatie aan het onthullen zijn. Anderzijds maken bronnen soms op onverwachte momenten gevoelige informatie openbaar, zonder dat de journalist daarop heeft kunnen anticiperen. Het kwaad is dan al geschied. Iedere vorm van onbeveiligd contact tussen bron en journalist laat een digitaal en dus herleidbaar spoor achter, met als risico dat iedereen die goed zoekt erbij kan (Henrichsen, 2020, pp. 338–339).

De ietwat pessimistische blik van journalisten op informatiebeveiligingstechnologie wordt niet alleen versterkt door onwetendheid, maar ook door een gevoel van onmacht. Het gevoel dat er simpelweg niet op te boksen valt tegen digitale spionage, helemaal als overheden en inlichtingendiensten erachter zitten (Bradshaw, 2017, p. 345; Kunert et al., 2022, p. 771). Journalisten raken ontmoedigd om zich te verdiepen in ingewikkelde informatiebeveiligings-technologieën en werken bovendien in een redactiecultuur die dit nauwelijks stimuleert. Digitale veiligheid heeft meestal geen prioriteit, wat met name wordt veroorzaakt door een gebrek aan kennis op bestuurlijk niveau. En hoewel de meeste nieuwsorganisaties een IT-

afdeling hebben, verloopt communicatie tussen journalisten en IT'ers vaak moeizaam, wat de succesvolle implementatie van digitale beveiligingstechnologie in de weg staat.

Ondanks alle obstakels zijn er voor journalisten genoeg redenen om digitale veiligheid serieus te nemen. Henrichsen (2020, p. 339-342) onderscheidt er drie: (1) zelfbescherming; (2) bescherming van het nieuwsverhaal; en (3) bescherming van de journalistieke waakhondfunctie. Opvallende afwezige in dit rijtje is de bescherming van bronnen, hoewel respondenten uit het onderzoek van Crete-Nishihata et al. (2020) dit wel weer benoemden. Diezelfde auteurs zagen bovendien een groot verschil in de perceptie op digitale bronbescherming tussen onderzoeksjournalisten en niet-onderzoeksjournalisten enerzijds en tussen journalisten in vaste dienst en freelancers anderzijds. Waar onderzoeksjournalisten en freelancers over het algemeen meer waarde hechten aan digitale veiligheid, achten niet-onderzoeksjournalisten dit vaak minder relevant en worden vaste stafleden bovendien gehinderd door de weinig stimulerende redactiecultuur waarin ze werken (Crete-Nishihata et al., 2020, pp. 1082–1084).

2.4. Surveillance en de relatie tussen journalisten en vertrouwelijke bronnen

In de eerste drie paragrafen uit het theoretisch kader is gekeken naar respectievelijk de omgang van journalisten met vertrouwelijke bronnen, de conceptuele ontwikkeling van het *chilling effect* en informatiebeveiligingstechnologie voor journalistieke bronbescherming. In het tweede deel van dit onderzoek worden deze drie thema's met elkaar samengebracht, zoals vergelijkbaar met de studies van onder meer Bradshaw (2017), Di Salvo, (2022) en Lashmar (2017). Eerstgenoemde onderzocht de impact van digitale surveillance op het werk van Britse regiojournalisten, vooral met betrekking tot de bescherming van vertrouwelijke bronnen. Di Salvo (2022) en Lashmar (2017) deden hetzelfde, maar richtten zich in plaats daarvan op onderzoeksjournalisten uit verschillende Westerse democratieën. De Nederlandse onderzoeksjournalistiek is in bestaande literatuur nog onderbelicht, maar zal aan de hand van dit onderzoek verder worden verkend.

In lijn met het theoretisch kader is ervoor gekozen om de rest van dit onderzoek te structureren aan de hand van drie deelvragen. Uit de eerste paragraaf blijkt dat het werken met anonieme bronnen journalisten in tweestrijd brengt. Het geeft journalisten vaak toegang tot vertrouwelijke informatie, maar is tegelijkertijd in strijd met journalistieke basisprincipes als objectiviteit, verificatie en transparantie. Hoe Nederlandse onderzoeksjournalisten omgaan met dit dilemma, zal aan de hand van de eerste deelvraag duidelijk moeten worden.

DV1: Hoe ervaren Nederlandse onderzoeksjournalisten het werken met anonieme bronnen en de daaraan verbonden ethische verplichting tot bronbescherming?

De tweede paragraaf uit de theorie gaat over de dreiging van overheidssurveillance en de impact daarvan op het gedrag van journalisten. Uit eerdere studies blijkt dat schrijvers en journalisten zich steeds meer bewust zijn van de surveillancepraktijken van overheden. Angst hiervoor kan leiden tot bevriezing. Denk aan journalisten die bijvoorbeeld stoppen met hun onderzoek, omdat ze niet langer in staat zijn de identiteit van vertrouwelijke bronnen te beschermen tegen digitale spionage. Of Nederlandse onderzoeksjournalisten een vergelijkbare angst ervaren, moet blijken uit de tweede deelvraag.

DV2: Hoe ervaren Nederlandse onderzoeksjournalisten de dreiging van overheids-surveillance en leidt dit bij hen tot een *chilling effect*?

De onthullingen van massasurveillance door Edward Snowden in 2013 hebben geleid tot een golf van nieuwe literatuur over dit onderwerp. Een deel daarvan richt zich op de vraag hoe journalisten zich kunnen beschermen tegen de surveillancepraktijken van overheden en inlichtingendiensten. Hieruit blijkt dat door een gebrek aan kennis, gevoel van onmacht of onderschatting van de gevaren, journalisten nog weinig gebruik maken van digitale informatiebeveiligingstechnologie. Of dit ook voor Nederlandse onderzoeksjournalisten geldt, is een vraag die op basis van de derde deelvraag zal worden beantwoordt.

DV3: In hoeverre gebruiken Nederlandse onderzoeksjournalisten informatie-beveiligingstechnologieën om digitale communicatie met anonieme bronnen te beschermen?

3. Methode

Dit onderzoek gaat over de ervaringen van onderzoeksjournalisten met digitale overheidssurveillance en hoe zij hierop anticiperen als het gaat om de bescherming van vertrouwelijke bronnen. Om die vraag te beantwoorden zijn semigestructureerde diepte-interviews afgenomen bij Nederlandse onderzoeksjournalisten die werkzaam zijn voor uiteenlopende nieuwsorganisaties en redacties. Een uitgebreide toelichting op deze methode is terug te vinden in paragraaf 3.1, waarin ook het selectieproces van de respondenten staat beschreven. In 3.2 wordt het data-analyseproces toegelicht. De laatste paragraaf bevat een korte toelichting op de betrouwbaarheid en validiteit van het onderzoek.

3.1. Dataverzameling

Met dit onderzoek is geprobeerd een gedetailleerd inzicht te krijgen in de ervaringen van Nederlandse onderzoeksjournalisten met surveillance en de invloed daarvan op hun omgang met anonieme bronnen. Het is een thema dat in de wetenschappelijke literatuur al veel aandacht heeft gekregen, met name sinds de openbaarmakingen van Edward Snowden in 2013. Zijn onthullingen gingen over de *Five Eyes* – een bondgenootschap tussen inlichtingendiensten uit Australië, Canada, Nieuw-Zeeland, het Verenigd Koninkrijk en de Verenigde Staten – dus is onderzoek hierover vaak gericht op deze landen. Over de surveillance- en spionagepraktijken van de Nederlandse overheid en de impact daarvan op de binnenlandse journalistiek is echter nog weinig literatuur beschikbaar. Terwijl ook in Nederland de inlichtingendiensten zich intensief bezighouden met het werk van journalisten, zo bleek uit onderzoek van *NRC*. Het is daarom van belang dit thema verder te onderzoeken en deze studie kan worden gezien als een eerste verkenning van het onderwerp in Nederlandse context.

3.1.1. Onderzoeksmethode

Binnen *journalism studies* is kwalitatief onderzoek gebruikelijk en daar is deze studie geen uitzondering op. In tegenstelling tot kwantitatief onderzoek, dat vaak gaat over harde data (cijfers en statistieken), is een kwalitatieve methodologie bij uitstek geschikt om emoties, gedrag en overtuigingen van mensen in kaart te brengen (Choy, 2014, p. 100). Omdat de onderzoeksvraag van deze studie gaat over dit soort zachte data, namelijk de individuele ervaringen van Nederlandse onderzoeksjournalisten met overheidssurveillance en de invloed daarvan op hun werkwijze, is een kwalitatieve benadering de meest logische keuze. Het nadeel

hiervan, zo schrijft Choy (2014, p. 101), is dat dergelijk onderzoek geen objectieve verifieerbare resultaten produceert, omdat persoonlijke ervaringen zich moeilijker laten generaliseren. Anderzijds geeft het de onderzoeker de gelegenheid om meer gedetailleerd op het onderwerp in te gaan, wat weer kan leiden tot unieke inzichten.

Interviews zijn een veel gebruikte methode voor het verzamelen van zowel harde als zachte data. De resultaten van deze studie zijn gebaseerd op semigestructureerde diepte-interviews. Anders dan bij gestructureerde interviews, die vaak worden gebruikt voor kwantitatief onderzoek en waarbij de onderzoeker een gestandaardiseerde vragenlijst naloopt, geven semigestructureerde vraaggesprekken een veel beter inzicht in persoonlijke ervaringen, standpunten en overtuigingen. Het is een interviewvorm die bestaat uit hoofdzakelijk open vragen en daarmee respondenten uitnodigt tot het geven van uitgebreide antwoorden en beschrijvingen. Doordat de structuur van het interview niet volledig vastligt, blijft er bovendien ruimte voor spontane vragen die voortkomen uit het dialoog tussen interviewer en geïnterviewde (DiCicco-Bloom & Crabtree, 2006, p. 315).

Over de feitelijke aard en omvang van surveillance door de Nederlandse overheid kunnen op basis van dit onderzoek geen uitspraken worden gedaan. Het doel was om een inzicht te krijgen in de subjectieve ervaringen van Nederlandse onderzoeksjournalisten. Kwalitatief onderzoek aan de hand van semigestructureerde diepte-interviews zijn geschikt om die te meten. Gedurende de interviews kregen respondenten de gelegenheid om hun antwoorden zorgvuldig te onderbouwen en persoonlijke ervaringen, opvattingen en gevoelens gedetailleerd te reconstrueren. De interpretatie van de resultaten zijn terug te vinden in hoofdstuk 4.

3.1.2. Topiclijst

De interviews zijn gestructureerd aan de hand van drie overkoepelende thema's: (1) de ervaringen van Nederlandse onderzoeksjournalisten met het werken met en beschermen van anonieme bronnen; (2) de ervaringen van Nederlandse onderzoeksjournalisten met (digitale) overheidssurveillance en de mogelijke impact daarvan op hun werk; en (3) de ervaringen van Nederlandse onderzoeksjournalisten met en hun perceptie op informatiebeveiligings-technologie. Omdat deze onderwerpen elkaar overlappen, werd tijdens de interviews wel eens afgeweken van die structuur. De thema's bleken vooral een handige kapstok op basis waarvan de interviewvragen konden worden geformuleerd. Deze vragen staan in de topiclijst in de bijlage.

De thema's en vragen voor de interviews zijn geformuleerd naar aanleiding van de theorie uit hoofdstuk 2. Het eerste deel ging over vertrouwelijke bronnen en bronbescherming.

Respondenten werden gevraagd naar hun ervaringen hiermee en welke afwegingen ze maken voordat ze met dit soort bronnen samenwerken. Enerzijds is bronvermelding namelijk een belangrijke professionele norm die de transparantie en verifieerbaarheid van journalistiek werk vergroot. Anderzijds zorgt het verlenen van anonimiteit ervoor dat journalisten verhalen kunnen vertellen die anders misschien nooit naar buiten zouden komen. Dat betekent ook dat journalisten verplicht zijn de identiteit van bronnen te beschermen aan wie ze vertrouwelijkheid hebben beloofd. De vragen waren erop gericht om te achterhalen hoe Nederlandse onderzoeksjournalisten in praktijk omgaan met die uitdaging.

Het tweede thema ging over overheidssurveillance en bronbescherming. Onthullingen van massasurveillance door Amerikaanse inlichtingendiensten hebben geleid tot een enorme hoeveelheid nieuwe literatuur over dit onderwerp. Daaruit bleek onder andere dat schrijvers en journalisten wereldwijd het gevoel hebben door hun eigen overheden in de gaten te worden gehouden. Met name bij (onderzoeks-) journalisten die zich bezig houden met gevoelige onderwerpen omtrent nationale veiligheid kan dit leiden tot een *chilling effect*. De vraag was dan ook of Nederlandse onderzoeksjournalisten vergelijkbare ervaringen hebben en in hoeverre dit hun werk belemmert. Of zij gebruik maken van informatiebeveiligingstechnologie om zichzelf te wapenen tegen digitale spionage, is een vraag die tijdens het derde en laatste thema aan bod kwam.

3.1.3. Sampling

Voor het selecteren van respondenten is gebruik gemaakt van de strategie van *purposive sampling*. Dat wil zeggen dat journalisten die in het kader van dit onderzoek zijn benaderd voor een interview, bewust zijn gekozen op basis van één of meerdere kenmerken. Doelgerichte steekproeven zijn waardevol, omdat de onderzoeker hiermee casussen kan kiezen die in staat zijn een dieper begrip van het onderzochte onderwerp te geven (Coyne, 1997, p. 624). Daarom is in deze studie gekozen voor een focus op onderzoeksjournalisten vanuit de redenering dat zij, in vergelijking tot ‘gewone’ journalisten, vaker onderzoek doen naar gevoelige onderwerpen en om die reden meer ervaring hebben met vertrouwelijke bronnen en informatiebeveiliging. Alle respondenten die aan dit onderzoek deelnamen, werken voor onafhankelijke ondezoeksjournalistieke platforms, op onderzoekende redacties van kranten, televisie- of radiozenders of hebben anderzijds ervaring in de onderzoeksjournalistiek.

Voor het selectieproces was het eveneens belangrijk dat de onderzoeksjournalisten op de een of andere manier bekend waren met thema’s omtrent nationale veiligheid, politie, justitie, inlichtingendiensten, (georganiseerde) criminaliteit, corruptie, etc. Zij zullen in het

bijzonder in de belangstelling staan van inlichtingen- en veiligheidsdiensten, omdat ze regelmatig werken met zeer vertrouwelijke of belastende informatie. Niet voor niets concludeerde Mills (2019, p. 704) dat onder deze groep journalisten de angst voor surveillance en een daaruit voortkomend *chilling effect* groot is. Zij lopen nu eenmaal meer risico. Om te voorkomen dat de groep potentiële respondenten te klein zou worden, zijn behalve de hierboven genoemde criteria verder geen eisen gesteld aan de sample. Dat betekent dat de uiteindelijke steekproef relatief heterogeen was op het gebied van demografie, arbeidssituatie en werkervaring. Een overzicht van alle respondenten is terug te vinden in tabel 1 op pagina 27.

Om de omvang van de sample te bepalen, is gekeken naar saturatie. Dit is het punt in de dataverzameling waarop geen nieuwe inzichten worden gedaan en gegevens zich beginnen te herhalen. Het verzamelen van extra data, dat wil zeggen het aantrekken van nieuwe respondenten, is overbodig omdat het de kwaliteit van het onderzoek niet langer verhoogt (Hennink & Kaiser, 2022, p. 2). De mate van verzadiging is beoordeeld tijdens het coderen van de getranscribeerde interviews. Met ieder interview nam het aantal nieuwe codes af, wat betekent dat de antwoorden van de respondenten veel overeenkomsten vertoonden. Op enkele uitschieters na bevestigde de homogeniteit van de coderingen dat een steekproefgrootte van tien respondenten voldoende was om waardevolle conclusies uit te trekken.

3.1.4. Ethische verantwoording

Thema's als overheidssurveillance en inlichtingendiensten kunnen bij respondenten gevoelig liggen. Om de risico's voor hen zo klein mogelijk te houden, is ervoor gekozen om alle onderzoeksjournalisten anoniem in het onderzoek te vermelden. Dat betekende in de meeste gevallen het achterwege laten van naam en werkgever. Bij voorkeur werden de gesprekken op locatie gevoerd, maar om praktische redenen is de helft van de interviews telefonisch afgenomen. Mocht een respondent vanuit veiligheidsoverwegingen andere bezwaren hebben, werd hier gehoor aan gegeven. Uiteindelijk zijn het de journalisten zelf die de risico's het beste kunnen inschatten.

De interviews zijn – op voorwaarde dat de geïnterviewden hiermee akkoord gingen – met de spraakrecorderapp van een smartphone (of met Call Recorder) opgenomen en daarna met de hand of met behulp van transcriptiesoftware omgezet naar tekst, afhankelijk van de kwaliteit van de audio. Uit privacyoverwegingen is erop gelet dat de naam van de respondent niet in de audio of transcripties zou voorkomen. De audio-opnames werden opgeslagen en bewaard in een vergrendelde map en zijn, samen met de transcripties, direct verwijderd na afronding van dit onderzoek.

Tabel 1. Kenmerken respondenten (*N*=10)

N	Geslacht	Bereik	Dienstverband	Redactietype	Onderzoekservaring
1	Vrouw	Nationaal	Freelance	Krant/radio/ TV/online	Misstanden bij overheidsinstanties, internationale fraude en corruptie
2	Man	Nationaal	Freelance	Krant/radio/ TV/online	Politie en justitie, veiligheid, privacy
3	Man	Nationaal	Vaste dienst	TV/online	Arbeidsmisstanden, buitenlandse inlichtingendiensten, defensie
4	Man	Nationaal	Vaste dienst	Radio/TV/ online	Divers
5	Man	Nationaal	Vaste dienst	Krant	Politie en justitie, georganiseerde misdaad
6	Man	Regionaal	Vaste dienst	Krant	Divers
7	Vrouw	Nationaal	Freelance	Krant/radio/ TV/online	Georganiseerde misdaad, internationale fraude en corruptie
8	Man	Nationaal	Vaste dienst	TV/online	Technologie
9	Man	Regionaal	Vaste dienst	Krant	Politie en justitie
10	Man	Nationaal	Vaste dienst	Krant/radio/ TV/online	(Georganiseerde) misdaad

3.2. Data-analyse

De getranscribeerde interviews vormen de kwalitatieve data van dit onderzoek. Die data is in grofweg drie stappen en met behulp van *Atlas.ti* gecodeerd. In tabel 2 hieronder is iedere stap toegelicht met een voorbeeld. Het onderbrengen van codes in codegroepen en categorieën kan alleen plaatsvinden door data voortdurend met elkaar te vergelijken. Boeije (2002, p. 393) noemt dit *Constant Comparative Method (CCM).* Het is een waardevol proces, omdat op die

manier grote hoeveelheden tekst kunnen worden gereduceerd tot een aantal sleutelconcepten. Een compleet overzicht van alle codes en codegroepen is terug te vinden in Appendix B op pagina 57.

Tabel 2. Fases in het codeerproces volgens de theorie van Boeije (2002, p. 395-297)

Fase	**Definitie**	**Voorbeeld**
Open codering	Het labelen van relevante passages met één of meer bijpassende codes	Passage uit het interview met respondent 2 (p. 34): " […] Ik heb mijn hele computer dicht getikt, ik zit op Firefox, ik zit achter een VPN en ik heb een adblocker en ik heb Privacy Badger erop zitten en zo. Heel veel websites werken nu niet meer zo lekker." Deze uitspraak is gelabeld met de code 'gebruiksonvriendelijk.'
Axiale codering	Het indelen van losse codes in codegroepen	De code 'Gebruiksonvriendelijk' is onderdeel van de codegroep 'Belemmeringen voor het gebruik van informatiebeveiligingstechnologie'
Selectieve codering	Het samenvoegen van codegroepen in overkoepelende categorieën	De codegroepen 'Belemmeringen voor het gebruik van informatiebeveiligingstechnologie' en 'strategieën voor het beveiligen van informatie' behoren beide tot de categorie 'Informatiebeveiligingstechnologie'

De methode die in deze studie wordt gebruikt, raakt aan wat Braun & Clark (2006, p. 79) *thematische analyse* noemen: een methode voor het identificeren, analyseren en rapporteren van patronen (thema's) binnen data. De auteurs maken daarbij onderscheid tussen twee vormen van thematische analyse, namelijk inductief of deductief. Inductieve data-analyse wil zeggen dat in de data gezocht wordt naar verbanden of afwijkende patronen, op basis waarvan de onderzoeker een nieuwe theorie zou kunnen formuleren. Het is een data gedreven, 'top-down' proces, waarbij de onderzoeker de data niet in een vooraf bepaalde codeerframe probeert te plaatsen, maar codes en thema's baseert op de data voorhanden (Braun & Clark, 2006, p. 83).

Deductieve analyse is het tegenovergestelde hiervan: een bestaande theorie wordt aan de hand van nieuwe data getest. In praktijk betekent dit dat de onderzoeker vooraf bepaalde codes of thema's heeft geformuleerd, waarna hij de data doorzoekt op fragmenten die daarop

aansluiten (Braun & Clarke, 2006, p. 84). Het testen van een mogelijk *chilling effect* bij Nederlandse onderzoeksjournalisten is een goed voorbeeld van een deductieve benadering. Hetzelfde geldt voor de theorie dat journalisten vaak uit onwetendheid, onmacht of onderschatting nog weinig gebruik maken van informatiebeveiligingstechnologie. De interviews uit dit onderzoek zijn dus op zowel inductieve als deductieve wijze geanalyseerd.

3.3. Betrouwbaarheid en validiteit

Dit onderzoek gaat over subjectieve ervaringen. Om die te onderzoeken, zijn diepte-interviews een geschikte methode. Het is belangrijk om op te merken dat de onderzoeker bij de interpretatie van subjectieve kwalitatieve data een centrale rol inneemt. Om de validiteit, ofwel de geldigheid van het onderzoek te vergroten, is ervoor gekozen om de tekst vóór definitieve afronding aan de respondenten te laten lezen. Dit wordt door Van IJzendoorn & Miedema (1986, p. 503) *communicatieve validiteit* genoemd. Wanneer zij zich niet herkenden in het geschetste beeld, werd de tekst aangepast. Ook tijdens het analyseren van de data en het schrijven van de resultaten is geprobeerd zo transparant mogelijk te zijn over denk- en werkwijze. Zo is het codeerproces inzichtelijk gemaakt voor mede-onderzoekers en zijn respondenten aan de hand van quotes ook zelf veel aan het woord gelaten.

De betrouwbaarheid van onderzoek wordt mede bepaald door de herhaalbaarheid ervan. Van IJzendoorn & Miedema (1986, p. 499-500) maken onderscheid tussen *technische* en *argumentatieve betrouwbaarheid*. Argumentatieve betrouwbaarheid gaat over herhaalbaarheid in de data-verzamelfase van een onderzoek. Voor deze studie bijvoorbeeld, is gekozen voor een vrij algemene topiclijst. Vragen zijn niet toegespitst op het individu, maar op de respondenten in het algemeen, waardoor de interviews gemakkelijk te reproduceren zijn.

Technische betrouwbaarheid daarentegen gaat over het data-analyseproces: zou een andere onderzoeker na het volgen van alle stappen tot dezelfde conclusies kunnen komen? Die kans is kleiner, omdat de onderzoeker een grote rol speelt in de interpretatie van de data. Hier wordt de link tussen betrouwbaarheid en validiteit duidelijk zichtbaar. Als onderzoeker is het daarom belangrijk om bewust te zijn van de eigen subjectieve rol, zodat niet alleen de betrouwbaarheid maar ook de geldigheid van het onderzoek kan worden vergroot.

4. Resultaten

Voor dit onderzoek zijn interviews afgenomen met in totaal tien Nederlandse onderzoeksjournalisten. De resultaten daarvan zijn in dit hoofdstuk samengevat. De paragrafen komen overeen met de thema's uit het theoretisch kader en de interviews. Ze gaan over de ervaringen van Nederlandse onderzoeksjournalisten met anonieme bronnen en de daaraan verbonden ethische verplichting tot bronbescherming (4.1); de perceptie van onderzoeksjournalisten op de mogelijke dreiging van overheidssurveillance en de impact daarvan op hun werk als journalist (4.2); en het gebruik van informatiebeveiligingstechnologie (4.3). In de conclusie (hoofdstuk 5) worden de resultaten met elkaar verbonden en kan zodoende een antwoord worden geformuleerd op de hoofdvraag.

4.1. Nederlandse onderzoeksjournalisten over anonieme bronnen en bronbescherming

Deze studie gaat over de vraag hoe onderzoeksjournalisten omgaan met vertrouwelijke bronnen op het moment dat zij mogelijk doelwit zijn van overheidssurveillance. Om die vraag te kunnen beantwoorden, is het allereerst van belang een inzicht te krijgen in de algemene ervaringen van Nederlandse onderzoeksjournalisten met anonieme bronnen, de journalistieke afweging die daaraan vooraf gaat en de professionele verantwoordelijkheid van bronbescherming die eraan verbonden is.

4.1.1. Anonieme bronnen: de drijvende krachten achter onderzoeksjournalistiek

Op basis van de interviews lijkt het erop dat werken met anonieme bronnen voor Nederlandse onderzoeksjournalisten eerder regel dan uitzondering is. "Meer wel dan niet" (resp. 3), "eigenlijk komt het bij ieder onderzoek wel voor" (resp. 1) of "ik denk dat ik in 90% van mijn onderwerpen en thema's werk met vertrouwelijke bronnen" (resp. 9), vertellen respondenten. Het gaat dan vooral om bronnen die voor de buitenwereld anoniem zijn, maar waarvan de identiteit wel bij de journalist zelf en/of de hoofdredacteur bekend is.

> "Ik zal pas iemand gebruiken als ik weet wat de identiteit is van die persoon. Maar in sommige gevallen kan die bron inderdaad, om wat voor reden dan ook, bedingen dat de anonimiteit voor anderen vertrouwelijk blijft. Maar het is in mindere mate ofzo. Ik vind het niet zo sterk. Ik probeer te voorkomen dat de bronnen anoniem zijn" (resp. 5, p. 60).

Bovenstaande quote is afkomstig van de enige respondent die niet als onderzoeksjournalist bekend staat – hij is verslaggever bij een landelijke Nederlandse krant – of verbonden is aan een onderzoeksredactie. Het zou een verklaring kunnen zijn voor het feit dat hij in vergelijking met collega-respondenten, relatief weinig ervaring heeft met anonieme bronnen. Tegelijkertijd benoemt hij hier ook direct het dilemma waar veel onderzoeksjournalisten mee worstelen wanneer ze werken met vertrouwelijke bronnen. Want zetten ze daarmee niet hun geloofwaardigheid op het spel?

> "Het is wel een principiële discussie hè, van moet je bronnen openbaar maken? Want je kunt natuurlijk heel veel toeschrijven aan anonieme bronnen, terwijl die bronnen misschien helemaal niet bestaan. Je moet dan maar vertrouwen dat de journalist die bron ook echt heeft" (resp. 2, p. 15).

In het werken met anonieme bronnen wordt van nieuwsconsumenten dus gevraagd te vertrouwen op de integriteit van een journalist of een medium. Desondanks zijn alle respondenten het erover eens dat journalisten nooit enkel en alleen mogen leunen op bronnen die bij het grote publiek onbekend willen blijven. De aanwezigheid van ondersteunend bewijsmateriaal, bijvoorbeeld in de vorm van belastende documenten of bronnen die wél met naam en toenaam informatie kunnen bevestigen, werd tijdens de interviews vaak genoemd als belangrijke voorwaarde voor anoniem brongebruik (zie ook figuur 1).

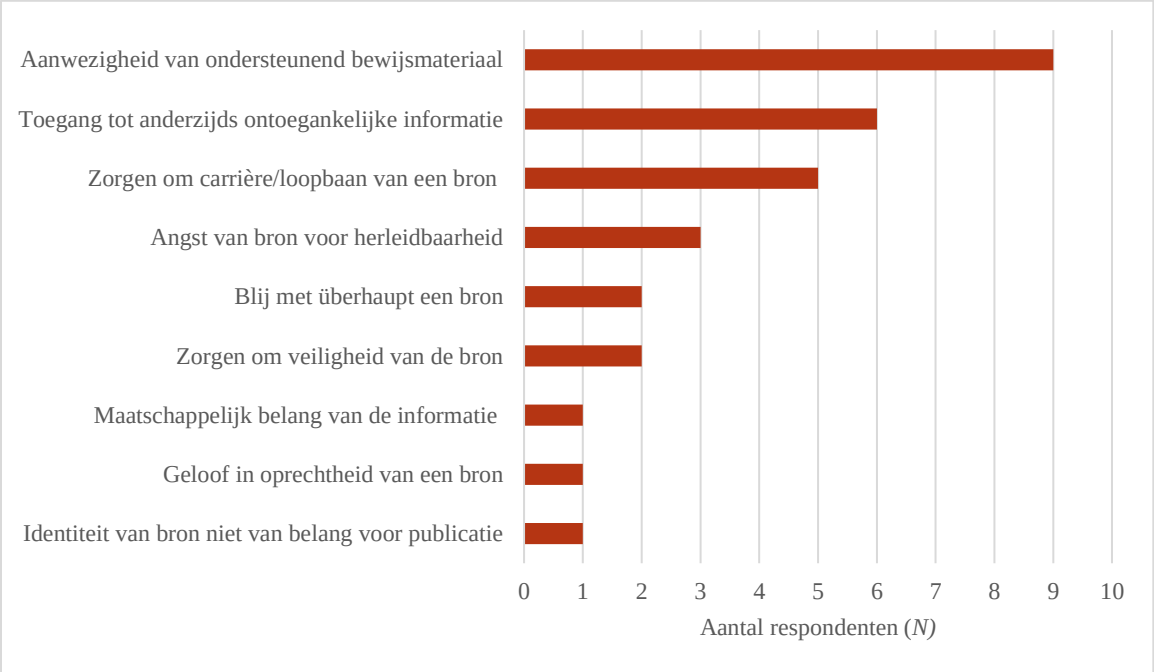
> "Het voordeel van onderzoeksjournalistiek is, denk ik, dat je meer tijd hebt om het allemaal te verifiëren aan de hand van openbare bronnen. Ik denk dat journalistiek dat over het algemeen wel doet hoor, maar ik denk dat wij als onderzoeksjournalisten daar gewoon net iets meer ruimte voor hebben, om het gat tussen een anonieme bron – en daarop vertrouwen – en openbare informatie, te dichten. En dan hoef je niet meer te zeggen dat je je baseert op een anonieme bron, omdat je eigenlijk alle informatie zelf al uit openbare informatie hebt weten te halen" (resp. 7, p. 86-87).

Toch is niet alle vertrouwelijke informatie direct te herleiden naar openbare bronnen. Klokkenluiders die staatsgeheimen onthullen bijvoorbeeld, zijn voor journalisten cruciaal om toegang te krijgen tot informatie die anderzijds nooit naar buiten zou komen. Eén van de respondenten zegt daarover: "Ik voelde me in die zin wel een beetje overvallen, dat ik ineens zo, bam!, staatsgeheimen in mijn gezicht kreeg. Dat ik dacht, jezus, dat is gewoon hartstikke strafbaar, die mag je helemaal niet hebben" (resp. 2, p. 18).

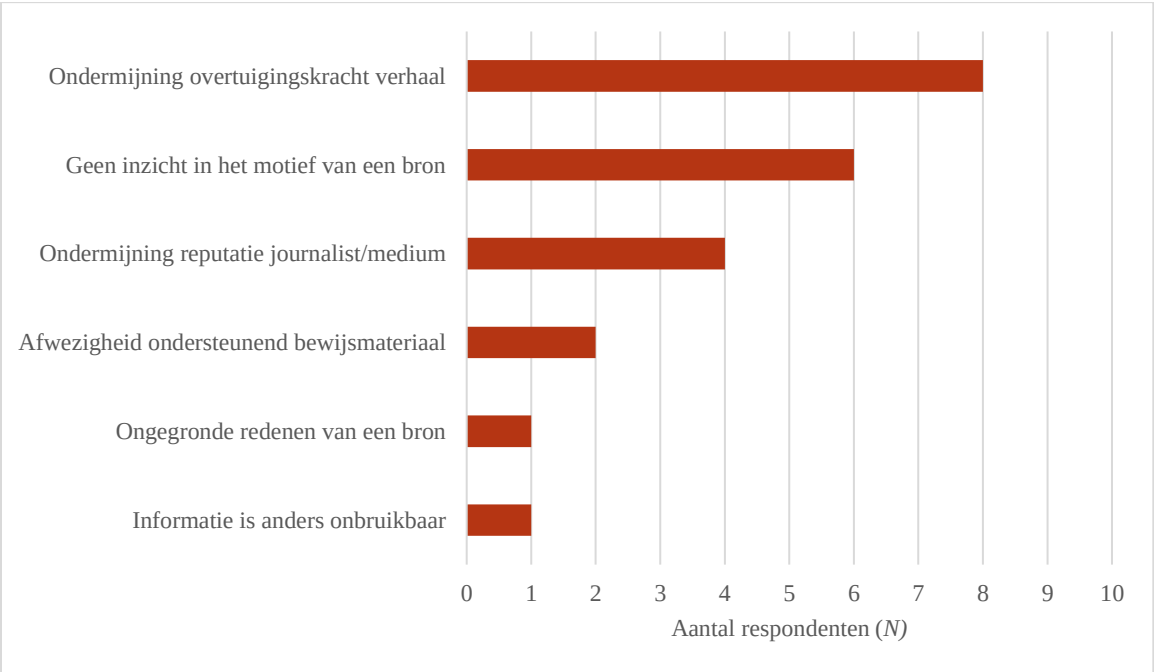
Waar vertrouwelijke of staatsgeheime bewijsstukken voor journalisten een goudmijn

zijn, lopen bronnen na het lekken van dergelijke informatie enorme risico's. Zorgen over hun loopbaan of veiligheid zijn voor hen redenen om anoniem te willen blijven. Dat betekent ook dat journalisten worden belast met een grote verantwoordelijkheid, namelijk het beschermen van de identiteit van bronnen aan wie zij vertrouwelijkheid hebben beloofd.

Figuur 1. Motieven voor journalisten om te werken met anonieme bronnen



Figuur 2. Motieven voor journalisten om niet te werken met anonieme bronnen



4.1.2. Bronbescherming: de heilige plicht van iedere journalist

Voor journalisten die werken met vertrouwelijke bronnen is bronbescherming heilig. Niet alleen omdat dit in het belang is van de veiligheid of bestaanszekerheid van hun bronnen, maar ook om hun eigen reputatie hoog te houden. Zelfs onder druk van de rijksrecherche of een rechter, met het risico mogelijk 'gegijzeld' te worden, is voor hen geen reden om terug te komen op de belofte die ze aan hun bronnen hebben gedaan.

> "Kijk, als jij ter plekke je bronnen gaat zitten verklappen, dan ben je natuurlijk weg. Dan denkt iedereen, oh, dus als die gast 24 uur in de cel zit, dan begint ie meteen…Maar dat gaat wel heel ver, ja" (resp. 2, p.18).

> "Ik ben wel eens onderdeel geweest van een onderzoek van de rijksrecherche. Die deed onderzoek naar het uitlekken van bepaalde details die in een verhaal van mij hebben gestaan. En daarbij ben ik toch wel regelmatig benaderd door die rechercheurs en later ook door de officier van justitie die dat onderzoek leidde, met het vriendelijke verzoek om in gesprek te treden. En dat had natuurlijk als doel, dat ik iets vertelde over mijn bronnen. Maar daar heb ik vriendelijk voor bedankt. Het is niet zo ver gekomen dat dat uiteindelijk een zaak werd. Of dat het voor een rechter komt. Maar ik ken wel collega's waar dat wel gespeeld heeft, ja" (resp. 10, p. 125).

Nederlandse onderzoeksjournalisten voelen over het algemeen een grote verantwoordelijkheid voor het beschermen van hun bronnen. In heel uitzonderlijke gevallen betekent dit het achterhouden van informatie voor politie en justitie, maar veel vaker zit die anonimiteit in het beschermen van bronnen tegen hun eigen werkgever of collega's.

> "De enige manier waarop je anonimiteit zou kunnen doorbreken, is dat je bijvoorbeeld de naam van die persoon wel noemt bij een ander persoon. Dat vind ik ook al een manier van bronbescherming. Als ik met bronnen praat, zeg ik ook nooit, ik heb ook met jouw collega gesproken. Omdat dat dan te herleidbaar is" (resp. 3, p. 39).

4.2. Nederlandse onderzoeksjournalisten over surveillance

Bronbescherming staat bij Nederlandse onderzoeksjournalisten hoog in het vaandel. Toch kan dit een stuk lastiger zijn wanneer inlichtingendiensten hen in het vizier hebben. Zoals in het voorbeeld van Stella Braam, die er in 2022 achter kwam dat de AIVD haar dertig jaar lang in de gaten had gehouden. Het maakte haar onzeker, omdat ze niet langer kon instaan voor de

veiligheid van haar bronnen. In deze paragraaf wordt onderzocht of de respondenten uit dit onderzoek vergelijkbare ervaringen hebben met overheidssurveillance en in hoeverre dit hun manier van werken en de omgang met vertrouwelijke bronnen beïnvloedt.

4.2.1. Gekraak op de lijn?

Voor alle geïnterviewden geldt dat zij op de hoogte zijn van de surveillancepraktijken van de Nederlandse overheid. Vaak omdat zij hierover hebben gelezen in de media – het verhaal van Stella Braam was bij de meeste onderzoeksjournalisten wel bekend – en soms ook uit persoonlijke ervaringen van collega's of eigen onderzoek naar de inlichtingenwereld. Toch hebben veruit de meeste respondenten zelf geen directe ervaringen gehad met overheidssurveillance.

> "Nou, ik weet dat het gebeurt natuurlijk. Ik lees de krant. Ik vraag me erg af of het bij mij ook zou gebeuren. Ik kan het me eigenlijk niet voorstellen. […] je hebt heel veel andere journalisten die interessanter zijn om te volgen. Dus ik denk niet dat het bij mij zou gebeuren. Maar, ja het zou ook niet totaal onwaarschijnlijk zijn eigenlijk" (resp. 1, p. 7).

Meerdere respondenten dachten geen doelwit te zijn van overheidssurveillance, bijvoorbeeld omdat hun werk niet interessant genoeg is – zoals in het geval van respondent 1 – of omdat ze nooit duidelijke signalen hebben gehad dat ze daadwerkelijk op de radar stonden van een inlichtingendienst. Dat wil overigens niet zeggen dat het helemaal niet gebeurt. "De overheid zal mij nooit laten weten dat ze me afluisteren" (respondent 4, p. 51). Anderzijds zijn veel onderzoeksjournalisten optimistisch over het feit dat de overheid niet zomaar naar deze middelen grijpt en dat het daarom over het algemeen wel meevalt met de surveillancepraktijken in Nederland.

> "Dat vertrouwen heb ik nog wel in de regelgeving in Nederland, dat in verreweg de meeste gevallen daar wel bescherming op zit. Wij zijn ook een beschermd beroep. Je kan niet zomaar journalisten gaan lopen tappen. Vandaar dat die zaak Stella Braam in het nieuws is gekomen" (resp. 9, p. 120).

> "Er zijn best grote drempels voor overheidsorganisaties om zoiets te doen bij journalisten. En als dat bekend wordt, dan is dat dan wel een schandaal meteen. Dus wat ik begrijp van mensen die het kunnen weten – van politie of inlichtingendiensten – ze doen het, ze doen het echt. Als ze het nodig vinden, dan

> doen ze het. Dus we zijn absoluut niet onaantastbaar ofzo. Maar ze doen het bij de doorsnee burger eerder dan bij journalisten. Dus ja, daar houd ik me maar aan vast" (resp. 4, p. 56).

Gevraagd naar hun kennis over de zaak Stella Braam benadrukken de meeste respondenten toch vooral de uitzonderlijkheid ervan. Geen van hen kan een vergelijkbare ervaring delen. Toch leeft onder een enkeling van hen wel het vermoeden dat er een keer is meegeluisterd.

> "Ja, dat gevoel heb ik wel gehad in het verleden. Maar ja, bewijs het maar eens. Ik bedoel, ik heb een periode gehad dat er rare tikken te horen waren tijdens telefoongesprekken. En dat gebeurde tijdens de research van een onderwerp dat wel, toch links had met inlichtingendiensten. Maar ja, je weet nooit of het waar is" (resp. 4 , p. 52).

> "Ik heb nooit bewijs gevonden van dat er surveillance heeft plaatsgevonden, in mijn geval. Ik heb wel een paar keer in mijn loopbaan het vermoeden gehad dat er werd meegeluisterd. […] Dat ik telefoontjes pleegde en […] dan hoorde je een klik op de lijn of in één keer was de verbinding verbroken. Dat ik dacht van hé, dit is toch wel gek. Maar dat zijn vermoedens" (resp. 9, p. 112).

Slechts één respondent heeft daadwerkelijk bewijs dat hij een keer is afgeluisterd. Niet omdat hij zelf doelwit was, maar omdat de bron met wie hij sprak wel op het lijstje van de opsporingsdiensten stond.

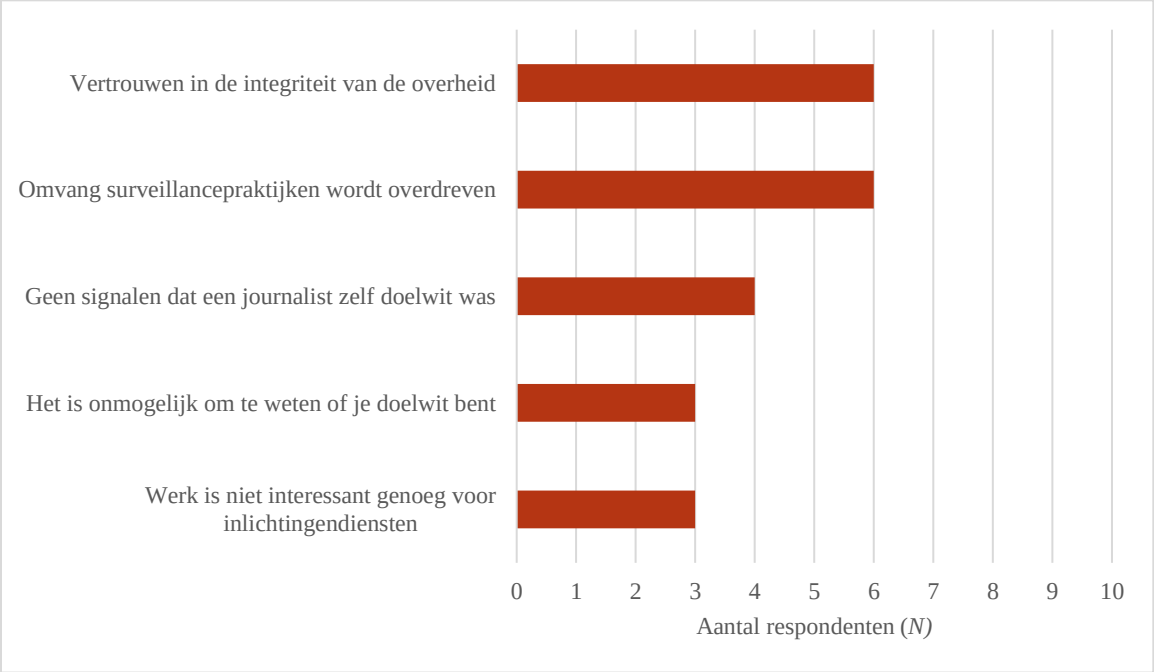
> "Ik heb ooit gesprekken gevoerd met personen die ook verdachte waren in een strafzaak. Daar was ik me van bewust, dat gesprek is getapt. En het OM heeft mij, zoals dat hoort, later er formeel op gewezen […] dat zij dat gesprek hebben afgeluisterd. Dat moeten zij ook doen. Ik was niet het onderwerp van de tap – dus dat mag ook – maar die verdachte en ik had daar een gesprek mee. Dus dat is het enige waarvan ik oprecht de surveillance van de overheid heb meegemaakt in een verhaal" (resp. 3, p. 40).

Een andere respondent zei wel eens aan tafel te hebben gezeten met de inlichtingendiensten:

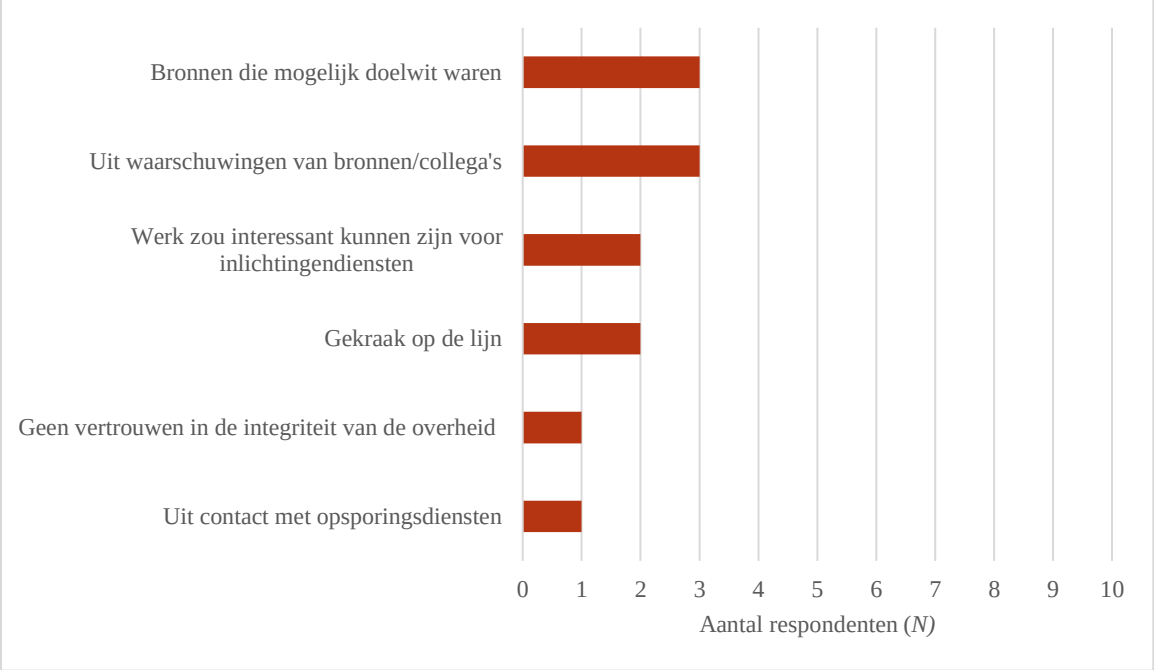
> "Kijk ik heb ook wel eens gesproken met mensen van de, dat heette toen nog de Criminele Inlichtingeneenheid van de politie, dat is nu Team Criminele Inlichtingen. Gewoon een achtergrondgesprek […] en aan het eind vragen ze dan ook, zou je eventueel voor ons willen werken? […] Ik ga ervan uit dat als ze zo'n

vraag stellen, dat ze dan ook wel iets uitgezocht zullen hebben. Maar ja, ik weet niet hoe paranoïde je moet worden" (resp. 2, p. 26).

Figuur 3. Waarom onderzoeksjournalisten geen directe ervaring hebben met overheidssurveillance



Figuur 4. Waarom onderzoeksjournalisten vermoedens hebben van overheidssurveillance



4.2.2. Paranoïde of naïef?

In tegenstelling tot wat in de literatuur wordt beschreven, leiden vermoedens van overheidssurveillance bij Nederlandse onderzoeksjournalisten niet direct tot een *chilling effect*. Dat zou, zo meent respondent 6 (p. 80) "heel ongezond zijn, als je [uit angst voor surveillance] al bij voorbaat zou zeggen: dan doe ik er maar niks mee." Niet publiceren is voor geen enkele journalist een optie. Liever passen ze hun werkwijze iets aan.

> "Nee, dat [overheidssurveillance] heeft er nooit toe geleid dat ik een onderwerp niet zou doen. En als ik er ook in de toekomst in terecht zou komen, in zo'n kwestie, in zo'n zaak, dan zal dat niet leiden tot stoppen met dat onderzoek of daar niet over publiceren, maar gewoon andere manieren van communicatie verzinnen" (resp. 9, p. 114).

Als het gaat om het aanpassen van hun werkwijze, zijn onderzoeksjournalisten creatief. De respondent van de quote hierboven bijvoorbeeld, vertelde hoe hij tijdens zijn onderzoek naar misstanden binnen de politie een zogenoemde pieper gebruikte om contact met zijn belangrijkste bron te onderhouden.

> "Ik denk wel dat ze hem [de bron] mogelijk afluisterden om te zoeken of hij mogelijk het lek was. Dat hebben we toen opgelost met een semafoon. Een oude pieper zeg maar, zoals ze in het ziekenhuis nog gebruiken. Toen hebben we die gekocht, eentje voor hem, eentje voor mij. […] Dus als ik dan hem bijvoorbeeld een berichtje stuurde, of hij mij – 1415307, ik noem maar wat – dan wist ik: dag één van de week, op de vierde plek die we hebben afgesproken, om half vier 's middags en dat cijfer daarna was dan van wel of niet nog iets van documenten meenemen. Zo'n systeem hebben we ooit gewoon live, ja buiten afgesproken. Daar stond niks van op papier. En dat was echt uit voorzorg, omdat ik er echt ernstig rekening mee hield dat in ieder geval hij werd afgeluisterd" (resp. 9, p. 113).

Voor een aantal respondenten is communicatie met 'gewone' bronnen eigenlijk nauwelijks anders dan met anonieme bronnen. Bij journalisten die wel hun werkwijze erop aanpassen, zit die verandering vooral in het gebruik van informatiebeveiligingstechnologie of in het terugvallen op analoge communicatie (zie paragraaf 4.3). En soms zijn het bronnen zelf die vragen om een andere werkwijze.

> "Ik heb ook wel bronnen bijvoorbeeld, bij de politie die gewoon alleen nog maar via Signal willen praten, omdat ze gewoon weten dat het niet gekraakt kan worden.

Dat weten ze zelf, omdat als een boef Signal heeft, dan kunnen ze dat ook niet kraken" (resp. 2, p. 19-20).

"Over het algemeen als iemand anoniem wil blijven, dan zeg je gewoon, je hebt mijn woord, dus dat komt goed. Ik zal nooit of te nimmer jouw naam aan iemand prijsgeven, ook niet als er om gevraagd wordt ofzo. En daar hou je je gewoon aan. En als dat vertrouwen dan wederzijds is, dan kun je gewoon bellen en mailen. Dan gaat dat wel goed. Maar er zijn mensen dus die zo voorzichtig zijn dat je er anders mee omgaat. Dus die willen alleen afspreken en dan ook inderdaad op een plek waar zo min mogelijk andere mensen zijn. Daar ga je dan in mee, maar dan meer om die wens van de ander te respecteren" (resp. 6, p. 81).

4.3. Nederlandse onderzoeksjournalisten over informatiebeveiligingstechnologie

Uit de vorige paragraaf werd duidelijk dat onderzoeksjournalisten soms hun manier van communiceren veranderen wanneer ze werken met vertrouwelijke bronnen en vermoeden dat dit contact interessant zou kunnen zijn voor externe partijen. In dat geval zijn er voor journalisten mogelijkheden om die communicatie extra te beveiligen, bijvoorbeeld door het gebruik van informatiebeveiligingstechnologie. In het derde en laatste deel van de interviews werd respondenten gevraagd naar hun ervaringen daarmee en hun perceptie op het werken met dergelijke tools. De resultaten daarvan zijn terug te lezen in deze paragraaf.

4.3.1. Zebrapaden tellen

Alle geïnterviewde onderzoeksjournalisten gebruiken informatiebeveiligingstechnologie om contact met vertrouwelijke bronnen te onderhouden, hoewel de frequentie en aard van het gebruik onder de respondenten flink verschilt. Veruit de meest genoemde tool is Signal, een versleuteld bel- en chatprogramma. Maar ook via Whatsapp kunnen journalisten en bronnen over het algemeen op een veilige manier met elkaar communiceren.

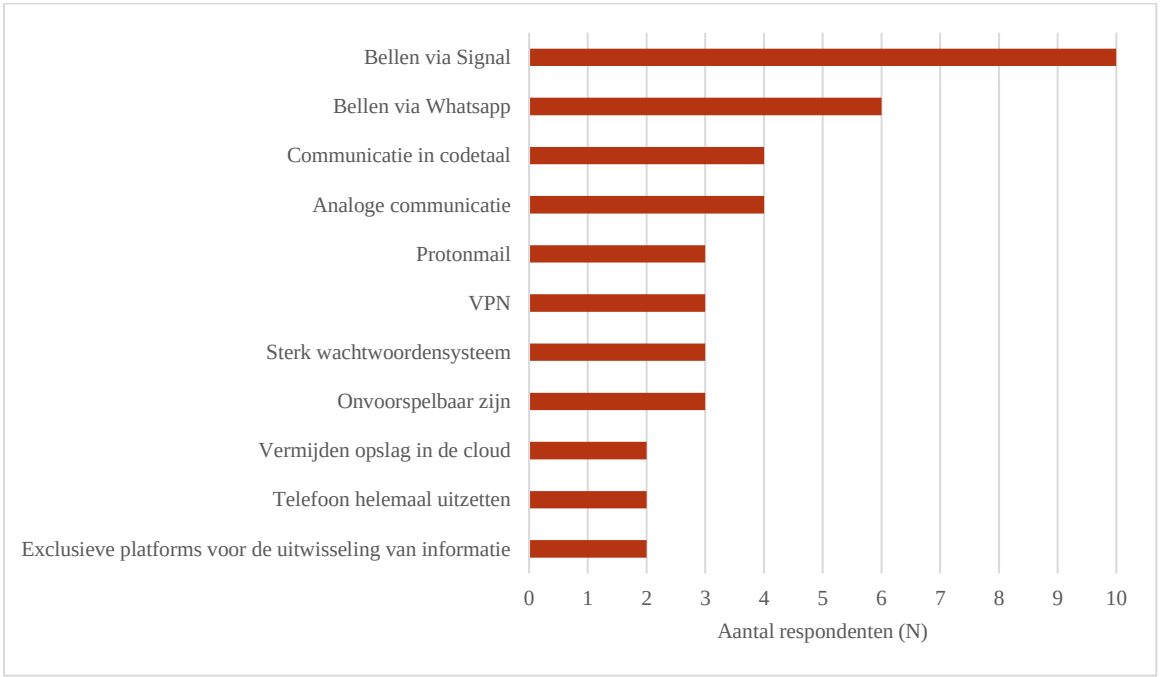
"WhatsApp is natuurlijk een versleutelde chatdienst en die gebruik je natuurlijk gewoon heel veel met bronnen, omdat dat gewoon een heel toegankelijk platform is wat veel in Nederland gebruikt wordt. Signal is voor bepaalde soorten bronnen ook wel een fijne manier om te communiceren, omdat die net iets minder informatie opslaat over wie met wie chat. En dat zijn eigenlijk twee hele toegankelijke apps waarmee je laagdrempelig contact kan hebben met bronnen op een manier die wel

zodanig versleuteld is, dat als het direct onderschept wordt dat het niet te belezen is" (resp. 8, p. 100).

Naast chatprogramma's als Signal zijn er voor journalisten ook versleutelde mailservers beschikbaar. Protonmail is daar een voorbeeld van. Dergelijke tools worden overigens niet alleen ingezet omdat journalisten dit zelf veiliger vinden, maar ook om bronnen gerust te stellen. Zo vertelt respondent 4 (p. 58): "Kijk, protonmail heeft een beetje de naam om heel veilig te zijn. Als ik daarmee bronnen zo ver kan krijgen dat ze toch wel communiceren met me, nou dan doen we het via protonmail. Ook goed weet je wel."

Figuur 5 geeft een overzicht van de meest gebruikte informatiebeveiligingsstrategieën door Nederlandse onderzoeksjournalisten. Het zijn strategieën, omdat het beveiligen van informatie zich voor de meeste journalisten niet alleen beperkt tot technologische hulpmiddelen als Signal of Protonmail. Een sterk wachtwoordensysteem bijvoorbeeld, kan al een groot verschil maken en in sommige gevallen gaan journalisten zelfs volledig over op analoge communicatie. Zoals respondent 4 (p. 52): "Ik heb mensen met wie ik alleen maar per post communiceer. Dan schrijven we alleen van 'koffie?' en dan weten we allebei waar we moeten afspreken."

Figuur 5. Meest genoemde informatiebeveiligingsstrategieën door Nederlandse onderzoeksjournalisten (*N*>2)



Bovengenoemde strategieën maken de communicatie met bronnen weliswaar veiliger, maar ze hebben ook een groot nadeel: het werk van journalisten wordt er een stuk ingewikkelder van.

> "Ik heb mijn hele computer dicht getikt… ik zit op Firefox, ik zit achter een VPN, ik heb een adblocker en ik heb Privacy Badger erop zitten en zo. Heel veel websites werken nu niet meer zo lekker. En dan denk ik, ja fuck, waarom werkt het nou niet? Ik zit maar te dreunen, waarom doet hij niks? Oh ja, omdat hij hem tegenhoudt. Bijvoorbeeld Google wil iedere keer van mij weten, ben jij geen robot? Moet ik iedere keer weer zebrapaden gaan tellen ofzo" (resp. 2, p. 34).

Het kost journalisten simpelweg ook gewoon heel veel tijd.

> "Kijk, weet je wat het probleem is vaak? Die extra beveiligde verbindingen, die zijn ook vaak tijdrovend om te installeren en te onderhouden en noem maar op. Terwijl je werk is ook vaak gebaat bij snelheid, dus dat staat een beetje op gespannen voet met elkaar" (resp. 4, p. 58).

Zo'n 70% van de respondenten noemde de gebruiksonvriendelijkheid een grote belemmering van het werken met informatiebeveiligingstechnologie. Een ander argument dat door een van de geïnterviewden werd aangehaald en ook overeenkomt met sommige bevindingen uit de literatuur, is het mogelijke afschrikeffect dat informatiebeveiligingstechnologie zou kunnen hebben op bronnen:

> "[…] je wil mensen ook niet bang maken. Als je zegt […] laten we protonmail gaan gebruiken…Eigenlijk zeg je dan tegen die persoon, nou ja misschien luisteren de diensten mee, je loopt gevaar. Snap je? Die indruk wil ik ook niet wekken, dus dan is het eigenlijk alleen maar nadelig om dat te doen" (resp. 3, p. 44).

4.3.2. Parels van Publeaks

Voor bronnen die anoniem een misstand willen melden, is er Publeaks: een online klokkenluidersplatform waar de meeste Nederlandse nieuwsredacties bij zijn aangesloten. Alle respondenten zijn bekend met het platform en meer dan de helft van hen vertelde ook wel eens te hebben gewerkt met bronnen die zich via Publeaks hadden gemeld.

> "Ik heb toevallig vanmiddag een telefoontje – het onderwerp noem ik even niet – maar wij zijn ook aangesloten op PubLeaks. Daar ben ik in contact gekomen met…dat is natuurlijk volledig anoniem, en daar ben ik over een tip nu in contact met iemand. En na wat mails over en weer hebben we nu telefoonnummers

> uitgewisseld en die ga ik vanmiddag spreken, telefonisch. Ik heb geen idee wie het is. Maar tegen de tijd dat we in zo'n geval met zo'n onderwerp verder gaan, ja uiteindelijk moet ik wel weten wie het is" (resp. 9, p. 106).

Communicatie via Publeaks gaat over de zwaarbeveiligde Tor-browser. Uit de interviews bleek dat de meeste nieuwsredacties één computer hebben die speciaal is aangesloten op Publeaks, waar 1 of 2 medewerkers van de redactie toegang tot hebben. Slechts één respondent vertelde verantwoordelijk te zijn voor het beheer van het Publeaks-account, de anderen kregen potentieel waardevolle informatie vaak doorgespeeld van hun collega. Hoewel het platform qua bronbescherming goed werkt, wordt er door journalisten ook veel over geklaagd.

> "[…] eerlijk gezegd zijn we daar niet heel positief over. […] het feit dat het zo drempelverhogend is, ook voor ons om toegang te hebben. Je moet dan eerst inloggen op een aparte computer en checken, etc. Nou ja, dat is een nadeel. Het is drempelverhogend want het wordt met meerdere media gedeeld. En doordat het algemeen bekend is, is negentig procent van wat er binnenkomt is onzin, dus daar moet je ook nog eens een keer doorheen […] Dus ik zou iets vergelijkbaars wat hetzelfde veiligheidsniveau heeft, maar dan alleen voor de [naam organisatie] zou werken ofzo, daar zou ik dan misschien wel een voorstander van zijn. Als het gewoon praktischer en toegankelijker is dan PubLeaks" (resp. 3, p. 45).

> "Het is natuurlijk een hartstikke fijn middel voor potentiële klokkenluiders om informatie te droppen. Tegelijkertijd is het ook een manier voor gekkies, om het zo maar even te zeggen, om de meest wilde complottheorieën te sturen. Dus je moet af en toe wel eens goed kijken wat er in zit en hoe je het moet wegen. Tegelijkertijd geldt dat natuurlijk voor iedere mailbox. Daar komt natuurlijk enorm veel binnen. En er zit wel eens een pareltje tussen. En vaak ook niet" (resp. 10, p. 128).

4.3.3. De macht van de tegenstander

Eerder deze paragraaf kwam naar voren dat het gebruik van informatiebeveiligingstechnologie voordelen en nadelen heeft. Ja, het maakt communicatie met bronnen enigszins veiliger, maar het werk van journalisten wordt er wel een stuk omslachtiger van. Om een inzicht te krijgen in de percepties van Nederlandse onderzoeksjournalisten op het belang van informatie-beveiligingstechnologie in hun werk, werd respondenten aan het einde van hun interview een viertal stellingen voorgelegd. De resultaten van drie daarvan zijn terug te lezen in tabel 2. De overige stelling zal in de lopende tekst worden toegelicht.

Tabel 3. Percepties van Nederlandse onderzoeksjournalisten op het belang van informatiebeveiligingstechnologie

Stelling	**Eens (*N*)**	**Oneens (*N*)**	**Totaal (*N*)**
Onderzoeksjournalisten moeten kunnen omgaan met informatiebeveiligingstechnologie	9	1	10
Onderzoeksjournalisten kunnen zichzelf nooit helemaal beschermen tegen hackers en digitale spionnen die in opdracht van de overheid werken	9	1	10
Informatiebeveiligingstechnologie is voor sommige onderzoeksjournalisten belangrijker dan voor andere	10	0	10

Het belang van kunnen omgaan met informatiebeveiligingstechnologie werd door bijna alle respondenten wel bevestigd. Experts hoeven ze niet te zijn, maar aan een zekere basiskennis kunnen onderzoeksjournalisten toch niet voorbijgaan, zo was een veelgehoord standpunt.

> "Ik vind niet dat elke journalist een diploma moet hebben met omgaan met de Tor browser en met encrypted mailen en zo. Dat vind ik onnodig. Maar als je met een zeer gevoelig onderwerp bezig bent, […] ja dan moet je er enige kennis van hebben en dan kun je niet volstaan met gewoon maar naïef je werk doen alsof je de dorpsverslaggever van … bent en een verhaal maakt over het 100-jarige jubileum van de harmonie. Dan moet je – dat vind ik dan wel onze professionele taak of plicht – toch wel even iets meer je erin verdiepen over hoe je een extra beschermingslaagje kunt inbouwen" (resp. 9, p. 121).

Eén respondent was minder overtuigd van het belang van informatiebeveiligingstechnologie voor het werk van journalisten. Zelf zei hij dergelijke tool nauwelijks te gebruiken.

> "Misschien doe ik er een beetje te laconiek over, maar het is wel cruciaal dat bronnen het gevoel hebben van, ja die kan ik vertrouwen. Maar ik geloof niet zozeer dat ze mij zouden vertrouwen, omdat ik nu heel goed duidelijk kan maken dat ik de nieuwste technieken heb waardoor ik op het internet niet te volgen ben. Of dat ik altijd heel encrypted communicatie verstuur" (resp. 5, p. 75).

Met welke soorten informatiebeveiligingstechnologie onderzoeksjournalisten overweg moeten kunnen, is volgens de geïnterviewden wel afhankelijk van het type onderzoek dat die persoon doet.

> "[…] naarmate de gevoeligheid van jouw onderzoek of jouw onderzoekdomein veel meer rijkt aan bijvoorbeeld de macht van de politie ofzo, dan wordt het natuurlijk wel een hele mate belangrijker om je goed te beschermen en je zaken op orde te hebben. Hoe machtiger de tegenstander, hoe beter je je moet beschermen" (resp. 8, p. 104).

Maar tegelijkertijd voelen respondenten ook: hoe machtiger de tegenstander, hoe lastiger die bescherming is. Daarom is 90% van de geïnterviewden het erover eens dat het onmogelijk is om volledig beschermd te zijn tegen overheidssurveillance. Als inlichtingendiensten bij je gegevens willen dan lukt dat ze toch wel, is de algemene gedachte. Al was één respondent het daar niet helemaal mee eens.

> "Ja ho…uiteindelijk zal de overheid er misschien wel bij kunnen komen, maar niet zonder zelf regels te overtreden. Dat is een belangrijke toevoeging. Er vanuit gaande dat de overheid dat niet doet – dat doen ze wel, ik wil niet naïef overkomen, maar laten we daar even vanuit gaan dat ze het niet doen – dan heb je als journalist voldoende mogelijkheden en middelen om daar omheen te werken. Het is heel simpel, wat ik net zei, als ik met iemand op de heide ga wandelen, ja dan zou ik niet kunnen bedenken hoe je kan worden afgeluisterd" (resp. 9, p. 120).

Informatiebeveiligingstechnologie zou onderzoeksjournalisten tot op zekere hoogte kunnen beschermen tegen spionnen en hackers van de overheid. De vraag is of het gebruik daarvan op redacties voldoende wordt gestimuleerd. Deze stelling is niet opgenomen in de bovenstaande tabel, omdat antwoorden hierop vaak wat genuanceerder lagen. Sommige respondenten waren heel stellig:

> "Ik vind echt dat het enorm onderschat wordt en […] ik zie dat het ook gewoon een klein beetje een generatieprobleempje is, met hoofdredacties die toch vaak wat ouder zijn en toch altijd wel structureel onderschatten wat de risico's zijn. Nee, ik vind niet dat dat [het gebruik van informatiebeveiligingstechnologie] gestimuleerd wordt. Eigenlijk bij alle redacties waar ik langskom vind ik dat dat niet echt het geval is" (resp. 7, p. 95).

De meesten waren wat genuanceerder of gaven aan weinig zicht te hebben op het redactiebeleid rondom informatiebeveiligingstechnologie:

> "Ja, weet ik eigenlijk niet. Nee, er zijn wel eens van die…dat heet dan nabespreking. Dan komt er iemand, een deskundige, die vertelt iets over dit of dat. Dat komt wel voor. Maar echt veel…nee" (resp. 5, p. 75).

Toch was zo'n 40-50% van de respondenten tevreden over het bewustzijn en beveiliging op de eigen redactie. En vaak zijn journalisten zich er zelf al van bewust, dus is stimuleren in sommige gevallen ook niet meer nodig.

> "[…] binnen onze krant, onze onderzoeksredactie, ja daar zijn we ons allemaal wel heel erg hiervan bewust. Maar daar hoeft het ook weer niet echt te worden gestimuleerd, want ik denk dat elk van mijn collega's zo ongeveer hetzelfde verhaal aan jou zou vertellen […]. Wij weten dat wel. Dus moet onze krant het nog meer stimuleren? Nee, dat gevoel heb ik niet meteen. En dat raakt een beetje aan van ja, plat gezegd, we moeten het ook niet overdrijven. We moeten alert zijn en er bedacht op zijn, maar moeten het ook niet overdrijven. Dat is mijn positie een beetje" (resp. 9, p. 121-122).

5. Conclusie en discussie

In dit onderzoek is naar een antwoord gezocht op de volgende vraag: Hoe ervaren Nederlandse onderzoeksjournalisten de mogelijke dreiging van digitale overheidssurveillance en hoe beïnvloedt dit hun werkwijze wat betreft de bescherming van vertrouwelijke bronnen? Er is gekeken naar (1) de ervaringen van onderzoeksjournalisten met anonieme bronnen en hun perceptie op de professionele verantwoordelijkheid tot bronbescherming; (2) de gevolgen van de dreiging van overheidssurveillance op het contact tussen bronnen en journalisten; en (3) het gebruik van en de perceptie op het belang van informatiebeveiligingstechnologie voor onderzoeksjournalisten. In dit hoofdstuk zijn de belangrijkste conclusies onder elkaar gezet, wordt een kritische blik geworpen op het onderzoeksproces en wordt gekeken naar mogelijkheden voor toekomstig onderzoek naar dit onderwerp.

5.1. Conclusie

Deze studie begon met een verkenning van de ervaringen van Nederlandse onderzoeksjournalisten met vertrouwelijke bronnen en hun perceptie op de daaraan verbonden ethische verplichting tot bronbescherming. Voor (bijna) alle respondenten is werken met anonieme bronnen heel normaal. Het zijn bronnen die toegang geven tot anderzijds onbereikbare informatie en daarmee van grote waarde zijn voor de onderzoeksjournalistiek. Journalisten die hun bronnen vertrouwelijkheid beloven, dragen de verantwoordelijkheid de identiteit van deze mensen te beschermen. Alle respondenten zagen het als hun professionele plicht om dit zo goed mogelijk te doen en geen van hen kon zich voorstellen ooit de belofte van bronbescherming te zullen breken. Een journalist zou daarmee niet alleen zijn eigen geloofwaardigheid, maar ook het algemeen vertrouwen in de journalistiek ondermijnen.

Bronbescherming wordt een stuk lastiger wanneer een journalist op de radar staat van overheden of inlichtingendiensten. Toen Stella Braam erachter kwam dat de AIVD haar jarenlang in de gaten had gehouden, durfde ze haar werk niet meer te doen. Bij haar trad een *chilling effect* op. Uit de interviews bleek dat die angst onder haar collega's wat minder leeft. Respondenten hebben over het algemeen weinig ervaring met overheidssurveillance en maken zich er dan ook niet direct zorgen over. Meer dan de helft van hen vertrouwt op het feit dat overheden niet zomaar journalisten mogen aftappen. Zij behoren immers tot een beschermde beroepsgroep. Niet voor niets kwam de zaak Stella Braam zo groot in het nieuws. Zulke verhalen zijn uitzonderlijk in Nederland en dus leeft onder de meeste onderzoeksjournalisten

het gevoel dat het over het algemeen wel meevalt met de surveillancepraktijken in Nederland.

Toch is het niet helemaal onwaarschijnlijk dat de overheid opsporingsbevoegdheden inzet ten koste van journalisten. Twee respondenten zeiden wel eens het vermoeden te hebben gehad dat er is meegeluisterd met hun telefoongesprekken, al hebben ze daar – behalve gekraak op de lijn – nooit hard bewijs voor kunnen vinden. Twee andere geïnterviewden vertelden aan tafel te hebben gezeten met de rijksrecherche of een inlichtingendienst, die hen probeerden te strikken voor een samenwerking. Beide journalisten wezen die uitnodiging af, maar realiseerden wel dat de opsporingsdiensten niet toevallig bij hen uit waren gekomen. Hoe meer journalistiek onderzoek raakt aan thema's als politie, justitie en inlichtingendiensten, hoe groter de dreiging van surveillance lijkt te worden.

Dat die dreiging kan leiden tot een *chilling effect*, zoals beschreven in de literatuur, daarvoor is in deze studie geen bewijs gevonden. Het zou in ieder geval voor geen van de respondenten een reden zijn om onderzoek te staken of niet te publiceren. Wel heeft het invloed op de manier waarop journalisten met hun bronnen communiceren en omgaan met de informatie die aan hen wordt gegeven. Van analoge communicatie tot praten in codetaal en van bellen via Signal tot mailen met behulp van Protonmail: respondenten benoemden talloze strategieën om contact zo anoniem mogelijk te houden voor de buitenwereld. Hoewel alle respondenten op de een of andere manier bekend waren met informatiebeveiligingstechnologie, merken zij ook: hoe zwaarder de beveiliging, hoe gebruiksonvriendelijker. Dus is een meerderheid, ondanks de noodzaak ervan, geen liefhebber van dergelijke tools.

Hoe ervaren Nederlandse onderzoeksjournalisten de mogelijke dreiging van digitale overheidssurveillance en hoe beïnvloedt dit hun werkwijze wat betreft de bescherming van vertrouwelijke bronnen? Uit tien gesprekken met Nederlandse onderzoeksjournalisten is gebleken dat de meeste van hen zich niet bedreigd voelen door de surveillancepraktijken van de overheid. Wel zijn alle respondenten zich ervan bewust dat het gebeurt. Dit bewustzijn beïnvloedt de manier waarop zij met hun bronnen communiceren. Beveiligde communicatieprogramma's zoals Signal zijn voor veel respondenten een belangrijk hulpmiddel. Maar goede bescherming gaat niet alleen over het gebruik van de nieuwste beveiligingstools. Belangrijker is dat journalisten discreet omgaan met de identiteitsgegevens van bronnen. Ingewikkelde technologieën schrikken bronnen enkel af en zijn bovendien toch niet opgewassen tegen de krachtige software van inlichtingendiensten. Dus is de mogelijke dreiging van overheidssurveillance voor de meeste onderzoeksjournalisten geen reden om hun werkwijze drastisch om te gooien.

5.2. Discussie en aanbevelingen

De respondenten die aan dit onderzoek hebben deelgenomen, zijn geselecteerd op basis van hun ervaringen met thema's als politie, justitie, inlichtingendiensten, corruptie en (georganiseerde) misdaad. Omdat er verder geen criteria waren, is het gelukt om een vrij divers sample samen te stellen gelet op werkomgeving en type redactie. Tijdens het coderen van de interviews bleek dat een grootte van tien respondenten voldoende was om een aantal algemene conclusies te kunnen trekken. De sample is echter te klein om volledig representatief te zijn. Aanvullend kwantitatief surveyonderzoek zou waardevol kunnen zijn om erachter te komen of de bevindingen uit dit onderzoek ook gelden voor de Nederlandse onderzoeksjournalistiek in het algemeen.

Het is belangrijk om te beseffen dat de respondenten uit deze studie over het algemeen veel ervaring hebben met thema's die sneller de belangstelling zullen wekken van overheidsdiensten. Misschien wel terecht merkten veel journalisten op dat het belang van informatiebeveiligings-technologie voor hen dan ook groter is dan voor collega's die bijvoorbeeld schrijven over zorg of klimaat. Of vergelijkbaar onderzoek onder andere respondenten dezelfde resultaten zal opleveren, is dus afhankelijk van de samenstelling van de sample. Tegelijkertijd biedt dit ook perspectief voor toekomstig onderzoek naar dit onderwerp. Hoe zit het bijvoorbeeld met de journalistiek in het algemeen of gelden de eerder getrokken conclusies enkel voor onderzoeksjournalisten? En is er verschil tussen journalisten die verbonden zijn aan regionale redacties en journalisten die werken voor nationale nieuwsmedia?

Dan nog een opmerking over de validiteit van het onderzoek. Omdat het ging om de persoonlijke ervaringen van Nederlandse onderzoeksjournalisten, is het lastig om de resultaten te beoordelen. Dat een journalist het gevoel heeft dat er wordt meegeluisterd met zijn of haar telefoongesprekken bijvoorbeeld, betekent niet dat dit daadwerkelijk gebeurt. En als journalisten het idee hebben dat het wel meevalt met de surveillancepraktijken in Nederland, wil dat niet zeggen dat ze naïef zijn. Misschien wordt de dreiging inderdaad flink overschat en is de casus van Stella Braam echt uitzonderlijk. Met andere woorden, de bevindingen van dit onderzoek zeggen niets over de daadwerkelijke omvang van surveillance door Nederlandse inlichtingen- en veiligheidsdiensten. De focus lag op de beleefwereld van onderzoeksjournalisten: hoe ervaren zij de dreiging van overheidssurveillance en welke implicaties heeft dit voor hun werk?

Op basis van gesprekken met Nederlandse onderzoeksjournalisten lijkt bewustzijn over de surveillancepraktijken van de Nederlandse overheid niet direct een ingrijpende invloed te

hebben op hun werkwijze. Dat het voorkomt betekent niet dat het bij hen ook gebeurt, merkten een aantal op. Meer dan de helft van de respondenten vertrouwt op de integriteit van de overheid. Een interessante conclusie vergeleken met Amerikaans onderzoek van Pew Research Center (2015), waaruit bleek dat 64% van de Amerikaanse onderzoeksjournalisten het vermoeden had dat de overheid gegevens over hun communicatie verzamelt. Dit weerhield hen er overigens niet van om hun onderzoek voort te zetten. Dat er in deze studie ook geen bewijs is gevonden voor een *chilling effect*, past dus in de lijn der verwachting.

De conclusie van Henrichsen (2020) dat weinig journalisten informatiebeveiligings-technologie gebruiken, wordt in deze studie tegengesproken. Uit interviews blijkt dat de meeste respondenten bewust bezig zijn met veilige communicatie, al ervaren zij bij het toepassen van technologische hulpmiddelen wel belemmeringen. Onder andere Kunert et al. (2022) en Waters (2018) schreven al over een gebrek aan technologische kennis, onderschatting van de risico's of twijfels over de effectiviteit van informatiebeveiligingstechnologie. Het zijn factoren die ook in dit onderzoek naar voren zijn gekomen en waaruit blijkt dat Nederland niet zo veel verschilt van zijn Westerse evenknieën.

Net als iedereen, zijn ook journalisten steeds meer afhankelijk van digitale communicatie. En daarmee zijn ze ook op een andere manier kwetsbaar geworden voor overheidssurveillance. Dat eigenlijk alle respondenten uit dit onderzoek zich bewust zijn van de risico's en hierop hun werkwijze kunnen aanpassen, lijkt een positieve ontwikkeling die past in het huidige tijdperk. Tegelijkertijd is het voor veel respondenten ook balanceren tussen paranoia en naïviteit. Waar sommigen tevreden zijn over hun eigen beveiliging en die van hun collega's, zijn andere respondenten van mening dat lang niet alle journalisten goed weten wat de gevaren zijn en hoe zij zich hier tegen kunnen beschermen. Het is een debat zonder winnaar, maar dat desalniettemin belangrijk is om te voeren. Met dit onderzoek is geprobeerd het belang daarvan te benadrukken en openingen te bieden voor toekomstig onderzoek.

Bibliografie

Berkowitz, D. A. (2009). Reporters and Their Sources. In K. Wahl-Jorgensen & T. Hanitzsch (Red.), *The handbook of journalism studies* (pp. 102–115). Routledge

Boeije, H. (2002). A Purposeful Approach to the Constant Comparative Method in the Analysis of Qualitative Interviews. *Quality & Quantity*, 36, 391–409.

Bradshaw, P. (2017). Chilling Effect: Regional journalists' source protection and information security practice in the wake of the Snowden and Regulation of Investigatory Powers Act (RIPA) revelations. *Digital Journalism*, 5(3), 334–352. https://doi.org/10.1080/21670811.2016.1251329

Büchi, M., Festic, N., & Latzer, M. (2022). The Chilling Effects of Digital Dataveillance: A Theoretical Model and an Empirical Research Agenda. *Big Data & Society*, 9(1), 1-14. https://doi.org/10.1177/20539517211065368

Carlson, M. (2009). Dueling, Dancing, or Dominating? Journalists and Their Sources. *Sociology Compass*, 3(4), 526–542. https://doi.org/10.1111/j.1751-9020.2009.00219.x

Choy L.T. (2014). The Strengths and Weaknesses of Research Methodology: Comparison and Complimentary between Qualitative and Quantitative Approaches. *IOSR Journal of Humanities and Social Science*, 19(4), 99-104. DOI: 10.9790/0837-194399104

Coyne, I.T. (1997). Sampling in qualitative research. Purposeful and theoretical sampling; merging or clear boundaries? *Journal of Advanced Nursing*, 26(3), 623-630. DOI: 10.1046/j.1365-2648.1997.t01-25-00999.x

Crete-Nishihata, M., Oliver, J., Parsons, C., Walker, D., Tsui, L., & Deibert, R. (2020). The Information Security Cultures of Journalism. *Digital Journalism*, 8(8), 1068–1091. https://doi.org/10.1080/21670811.2020.1777882

Deuze, M. (2005). What is journalism? Professional identity and ideology of journalists reconsidered. *Journalism*, 6(4), 442–464. https://doi.org/10.1177/1464884905056815

Di Salvo, P. (2021). Securing Whistleblowing in the Digital Age: SecureDrop and the Changing Journalistic Practices for Source Protection. *Digital Journalism*, 9(4), 443 460. https://doi.org/10.1080/21670811.2021.1889384

Di Salvo, P. (2022). "We Have to act Like our Devices are Already Infected": Investigative Journalists and Internet Surveillance. *Journalism Practice*, 16(9), 1849–1866. https://doi.org/10.1080/17512786.2021.2014346

DiCicco-Bloom, B., & Crabtree, B. F. (2006). The qualitative research interview. *Medical*

Education, 40, 314–321. https://doi.org/10.1111/j.1365-2929.2006.02418.x

Dohmen, J. (2022a, 28 augustus). AIVD hield onderzoeksjournalist 35 jaar in de gaten—En liet huisgenoot haar bespioneren. *NRC*. https://www.nrc.nl/nieuws/2022/08/28/aivd hield onderzoeksjournalist-35-jaar-in-de-gaten-en-liet-huisgenoot-haar-bespioneren a4139991

Dohmen, J. (2022b, 14 oktober).De AIVD beschermt de staatsveiligheid, maar brengt journalisten in gevaar. *NRC*. https://www.nrc.nl/nieuws/2022/10/14/de-aivd beschermt-de-staatsveiligheid-maar-brengt-journalisten-in-gevaar-a4145056

Duffy, M. J. (2014). Anonymous Sources: A Historical Review of the Norms Surrounding Their Use. *American Journalism*, 31(2), 236–261. https://doi.org/10.1080/08821127.2014.905363

Duffy, M. J., & Freeman, C. P. (2011). Unnamed Sources: A Utilitarian Exploration of their Justification and Guidelines for Limited Use. *Journal of Mass Media Ethics*, 26(4), 297-315. https://doi.org/10.1080/08900523.2011.606006

Evers, H. (2011). *Kan dat zomaar? Over ethische kwesties in de journalistiek*. Boom Lemma Uitgevers.

Hennik M., & Kaiser, B.N. Sample sizes for saturation in qualitative research: A systematic review of empirical tests. *Social Science & Medicine*, 292, 1-10. DOI: 10.1016/j.socscimed.2021.114523

Henrichsen, J. R. (2020). Breaking Through the Ambivalence: Journalistic Responses to Information Security Technologies. *Digital Journalism*, 8(3), 328–346. https://doi.org/10.1080/21670811.2019.1653207

Kunert, J., Frech, J., Brüggemann, M., Lilienthal, V., & Loosen, W. (2022). How Investigative Journalists Around the World Adopt Innovative Digital Practices. *Journalism Studies*, 23(7), 761–780. https://doi.org/10.1080/1461670X.2022.2033636

Lashmar, P. (2017). No More Sources?: The impact of Snowden's revelations on journalists and their confidential sources. *Journalism Practice*, 11(6), 665–688. https://doi.org/10.1080/17512786.2016.1179587

Martijn, M., & Tokmetzis. (2016). *Je hebt wél iets te verbergen. Over het levensbelang van privacy*. De Correspondent.

Martin-Kratzer, R., & Thorson, E. (2007). Use of Anonymous Sources Declines in U.S. Newspapers. *Newspaper Research Journal*, 28(2), 56–70. https://doi.org/10.1177/073953290702800204

McGregor, S. E. (2014). *Digital Security and Source Protection for Journalists (*Tow Center

for Digital Journalism Publications). Tow Center for Digital Journalism, Columbia University. https://doi.org/10.7916/D89P3D4M

Mills, A. (2019). Now You See Me – Now You Don't: Journalists' Experiences With Surveillance. *Journalism Practice*, 13(6), 690–707. https://doi.org/10.1080/17512786.2018.1555006

Modderkolk, H. (2022). *Het is oorlog maar niemand die het ziet*. Uitgeverij Podium.

Nederlands Genootschap van Hoofdredacteuren. (2008). Code voor de journalistiek. www.genootschapvanhoofdredacteuren.nl/. https://genootschapvanhoofdredacteuren.nl/code-voor-de-journalistiek/

PEN American Center. (2015). *Global Chilling: The Impact of Mass Surveillance on International Writers* [PEN's International Survey of Writers]. https://pen.org/research-resources/global-chilling/

Penney, J. (2021). Understanding Chilling Effects. *Minnesota Law Review*, 106(1451), 1451 1530. https://doi.org/10.2139/ssrn.3855619

Pew Research Center. (2015). *Investigative Journalists and Digital Security. Perceptions of Vulnerability and Changes in Behavior.* https://www.pewresearch.org/journalism/2015/02/05/investigative-journalists-and digital security/

Posetti, J. (2017). *Protecting Journalism Sources in the Digital Age*. UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000248054

Reich, Z. (2006). The process model of news initiative. Sources lead first, reporters thereafter. *Journalism Studies*, 7(4), 497-514. https://doi.org/10.1080/14616700600757928

Schauer, F. (1978). Fear, Risk and the First Amendment: Unraveling the Chilling Effect. *Boston University Law Review*, 58(685), 685-732.

Shapiro, I., Brin, C., Bédard-Brûlé, I., & Mychajlowycz, K. (2013). Verification as a Strategic Ritual, How journalists retrospectively describe processes for ensuring accuracy. *Journalism Practice*, 6(7), 657–673. https://doi.org/10.1080/17512786.2013.765638

Smith, R. F. (2007). Impact of Unnamed Sources on Credibility Not Certain. *Newspaper Research Journal*, 28(3), 8–19. https://doi.org/10.1177/073953290702800302

Solove, D. J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review*, 154(3), 477-560. https://doi.org/10.2307/40041279

Solove, D. J. (2021). The Myth of the Privacy Paradox. *George Washington Law Review*, 1(89), 1–51.

Sternadori, M. M., & Thorson, E. (2009). Anonymous Sources Harm Credibility of All

Stories. *Newspaper Research Journal*, 30(4), 54–66. https://doi.org/10.1177/073953290903000405

Townend, J. (2017). Freedom of Expression and The Chilling Effect. In H. Tumber & S. Waisbord (Red.), *The Routledge Companion to Media and Human Rights* (pp. 73–82). Routledge.

Van Aelst, P., & Vliegenthart, R. (2014). Studying the Tango: An analysis of parliamentary questions and press coverage in the Netherlands. *Journalism Studies*, 15(4), 392–410. https://doi.org/10.1080/1461670X.2013.831228

Van IJzendoorn, M.H., & Miedema, S. (1986). De kwaliteit van kwalitatief onderzoek. Pedagogischc Studien, (63), 498-505.

Verlaan, D. (2020). *Ik weet je wachtwoord. Waargebeurde verhalen over de duistere kant van het internet.* (Tweede druk). Das Mag Uitgevers.

Vobič, I., & Kovačič, M. P. (2015). Watchdog journalism and confidential sources: A study of journalists' negotiation of confidentiality with their sources. *Teorija in Praksa*, (52)4, 591-611.

Waters, S. (2018). The Effects of Mass Surveillance on Journalists' Relations With Confidential Sources: A constant comparative study. *Digital Journalism*, 6(10), 1294-1313. https://doi.org/10.1080/21670811.2017.1365616

Appendix A. Topiclijst interview

In deze bijlage is de topiclijst voor de semigestructureerde diepte-interviews uitgewerkt. Het doel van deze interviews is om inzicht te krijgen in de ervaringen van Nederlandse onderzoeksjournalisten met de mogelijke dreiging van overheidssurveillance en de manier waarop dit hun werkwijze wat betreft de omgang met vertrouwelijke bronnen beïnvloedt. De topiclijst bestaat uit drie onderdelen die corresponderen met de thema's uit het theoretisch kader: (1) vertrouwelijke bronnen en bronbescherming; (2) surveillance en het chilling effect; en (3) gebruik van en perceptie op informatiebeveiligingstechnologie. Ieder onderdeel bestaat uit de volgende elementen:

- **Doelstelling**. Dit is de hoofdvraag van ieder onderdeel en komt overeen met een van de drie deelvragen uit paragraaf 2.4.
- **Interviewvraag**. Een aantal vooraf opgestelde vragen die helpen bij het structureren van het interview en moeten leiden tot een antwoord op de deelvraag.
- **Aspecten om op door te vragen**. Dit zijn trefwoorden of korte zinnen aan de hand waarvan verdiepende vervolgvragen kunnen worden gesteld.

Voorbereiding van het interview

Voordat het interview echt van start kan gaan, is het belangrijk om de volgende stappen te doorlopen:

- Stel jezelf voor. Geef je naam en functie (student MA Journalistiek en Nieuwe Media) en vertel met welk doel je de interviews afneemt.
- Verzamel algemene informatie over de respondenten, zoals naam, bij welke nieuwsorganisatie ze werken, in welk type dienstverband (freelance of vaste loondienst) en aan welke onderzoeken ze hebben gewerkt of momenteel werken.
- Vertel respondenten hoe het interview eruit gaat zien. Laat weten dat het veelal open vragen zijn en dat het gaat om hun persoonlijke ervaringen. Moedig de respondenten aan tot het geven van uitgebreide antwoorden.
- Vraag de respondenten of ze met naam in het onderzoeksverslag mogen worden opgenomen. Geef hen de keuze om anoniem te blijven als zij zich hier veiliger bij voelen.
- Vraag vooraf toestemming voor het auditief opnemen van het interview. Gebruik anders pen en papier om de antwoorden van de respondenten te kunnen noteren.

Deel 1: Vertrouwelijke bronnen en bronbescherming

Doelstelling: Hoe ervaren Nederlandse onderzoeksjournalisten het werken met vertrouwelijke bronnen en de daaraan verbonden ethische verplichting tot bronbescherming?

Tabel I. Topiclijst bij deelvraag 1

Interviewvraag	Aspecten om op door te vragen
Heeft u wel eens gewerkt met vertrouwelijke bronnen?	**Ja**: vraag of de identiteit van deze bronnen wel (of niet) bekend was bij de journalist; **Nee**: vraag of die situatie zich nooit heeft voorgedaan of dat de journalist dit bewust heeft geweigerd;
Welke factoren spelen een rol wanneer u besluit een bron anonimiteit te geven?	Vraag naar de afweging tussen professionele normen als *objectiviteit*, *verificatie* en *transparantie* versus verkrijgen van vertrouwelijke informatie/veiligheid van de bron;
Vindt u dat anoniem brongebruik de geloofwaardigheid van de journalist zou kunnen aantasten?	Misbruik door de journalist (VB: fabriceren van bronnen); Misbruik door de bron (VB: anonimiteit om aansprakelijkheid te ontduiken);
Hoe kijkt u naar de ethische journalistieke code van bronbescherming?	Vraag respondenten of zij vinden dat dit een wettelijk recht zou moeten zijn;
Heeft u wel eens anonimiteit beloofd, maar om een of andere reden deze belofte moeten verbreken?	**Ja**: vraag naar de redenen en afwegingen (VB: belang van nationale veiligheid? Onder druk van een rechter?); **Nee**: vraag of die situatie zich nooit heeft voorgedaan of dat de journalist dit bewust heeft geweigerd;

Deel 2: Surveillance en het *chilling effect*

Doelstelling: Hoe ervaren Nederlandse onderzoeksjournalisten de dreiging van overheids-surveillance en leidt dit bij hen (en hun bronnen) tot een *chilling effect*?

Tabel II. Topiclijst bij deelvraag 2

Interviewvraag	Aspecten om op door te vragen
Bent u op de hoogte van of heeft u ervaring met surveillancepraktijken van de overheid?	Vraag naar voorbeelden/concrete ervaringen; vraag of respondenten bekend zijn met de case van Stella Braam of andere vergelijkbare gevallen; vraag welk gevoel de wetenschap van overheidssurveillance bij de respondenten oproept;
Heeft kennis over het voorkomen van overheidssurveillance u er wel eens van weerhouden om een verhaal te publiceren?	Vraag naar voorbeelden/concrete ervaringen;
Heeft kennis over het voorkomen van overheidssurveillance op een andere manier wel eens uw werkwijze beïnvloed?	Vraag naar voorbeelden/concrete ervaringen (VB: zelfcensuur, verwijderen van archiefmateriaal, vermijden van digitale communicatie met bronnen, etc.);
Heeft kennis over het voorkomen van overheidssurveillance bronnen er wel eens van weerhouden om mee te werken aan een onderzoek?	Vraag naar voorbeelden/concrete ervaringen; Vraag hoe respondenten hiermee omging;

Deel 3: Gebruik van en percepties op informatiebeveiligingstechnologie

Doelstelling: In hoeverre gebruiken Nederlandse onderzoeksjournalisten informatie-beveiligingstechnologieën om digitale communicatie met anonieme bronnen te beschermen?

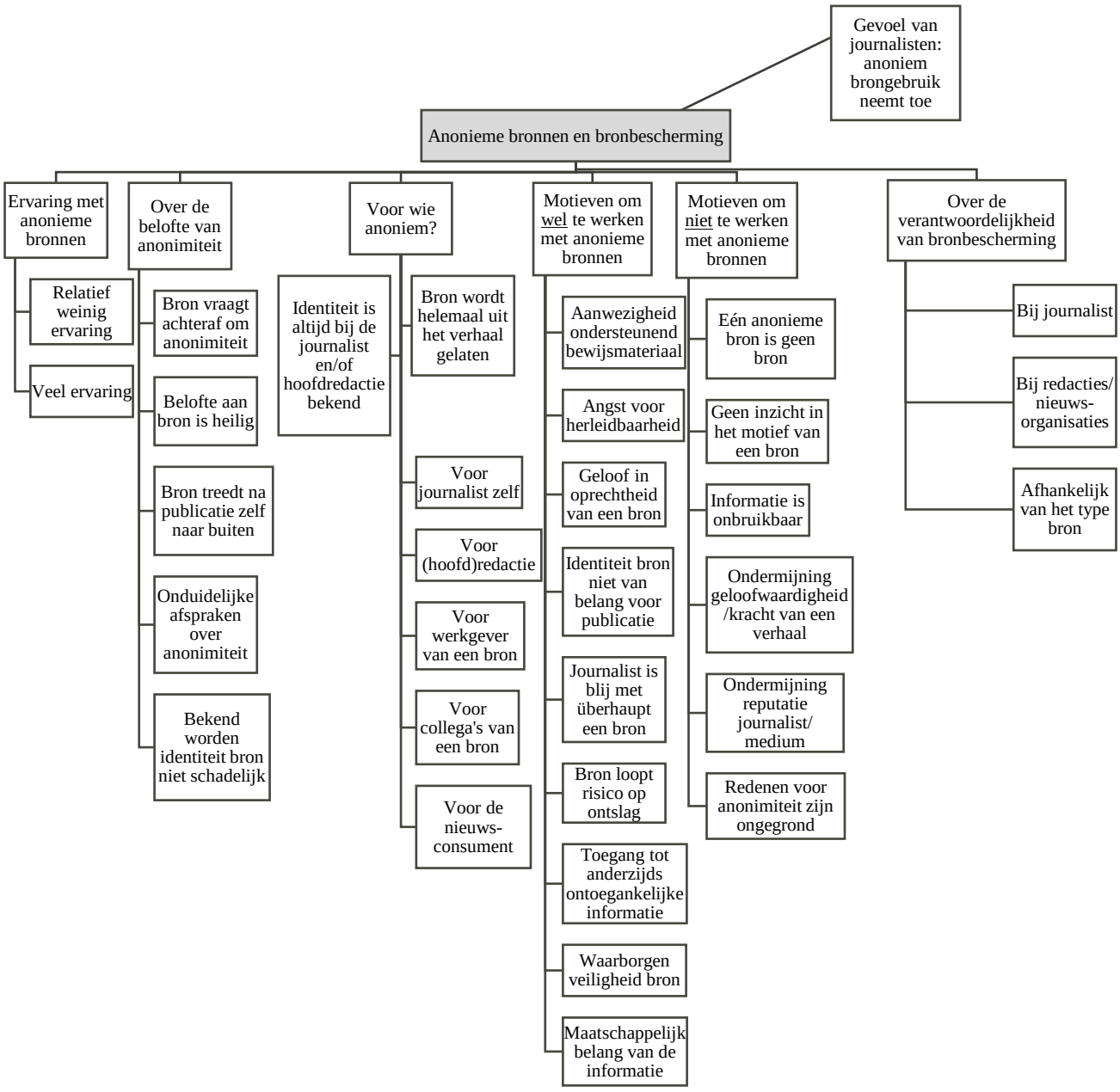
Tabel III. Topiclijst bij deelvraag 3

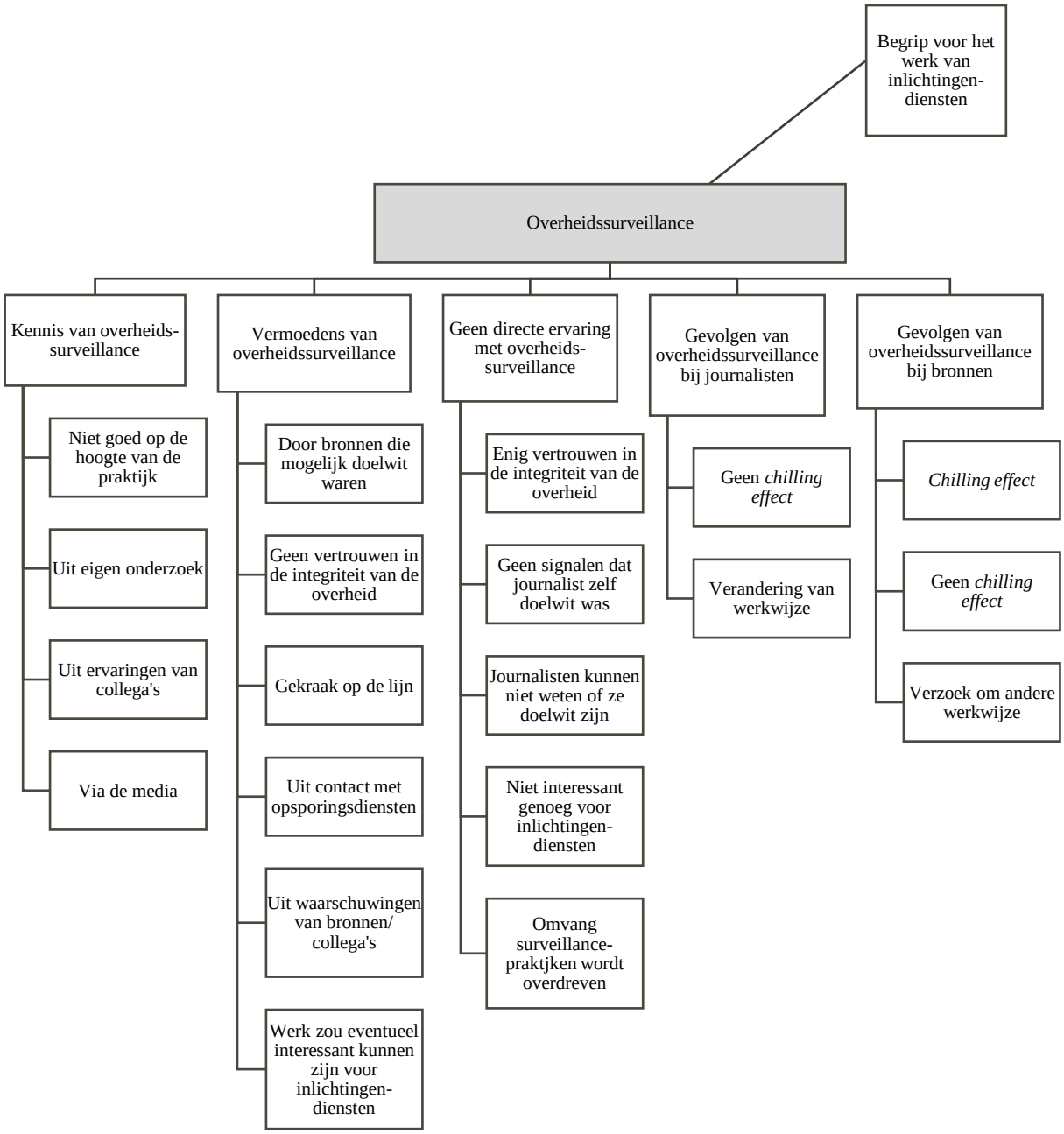
Interviewvraag	Aspecten om op door te vragen
Hoe verloopt communicatie/contact met bronnen over het algemeen?	Vraag naar de aard van het contact (digitaal, bijv. Whatsapp of e-mail, of fysiek);
In hoeverre is communicatie met anonieme bronnen anders dan met 'gewone' bronnen?	Vraag naar voorbeelden;
Heeft kennis over het voorkomen van overheidssurveillance uw communicatie met vertrouwelijke bronnen wel eens veranderd?	Vraag naar voorbeelden (VB: face-to-face contact i.p.v. online);
Gebruikt u wel eens informatie-beveiligingstechnologie wanneer u communiceert met (vertrouwelijke) bronnen?	Ja: vraag naar voorbeelden van informatiebeveiligingstechnologie (VB: versleuteld e-mailverkeer, vermijden van cloudopslag, installeren van anonieme webbrowsers); vraag wanneer de respondent hiermee begonnen is Nee: vraag naar de redenen daarvoor;
Bent u bekend of heeft u wel eens gewerkt met softwareplatforms als *PubLeaks*?	Vraag naar voorbeelden/concrete ervaringen;

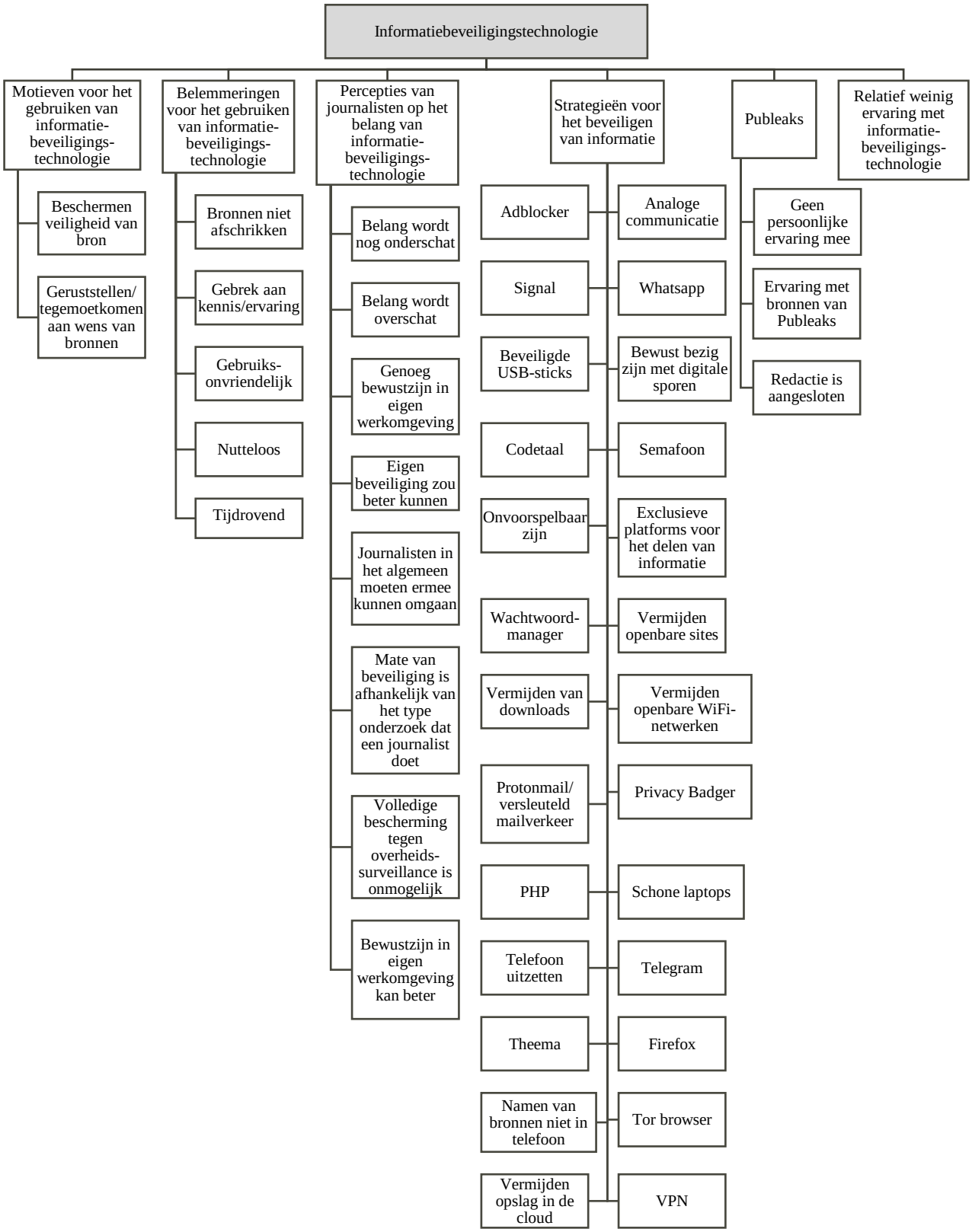
Leg de volgende **stellingen** voor aan de respondenten. In hoeverre zijn ze het hier mee eens of oneens? Vraag naar persoonlijke ervaringen en voorbeelden.

1) Onderzoeksjournalisten moeten kunnen omgaan met informatie-beveiligingstechnologie;
2) Onderzoeksjournalisten kunnen zichzelf nooit helemaal beschermen tegen hackers en digitale spionnen die in opdracht van de overheid werken;
3) Informatiebeveiligings-technologie is voor sommige onderzoeksjournalisten belangrijker dan voor anderen;
4) Redacties van nieuwsorganisaties stimuleren het implementeren van informatie-beveiligingstechnologie onvoldoende;

Appendix B. Codebomen




Begrip voor het werk van inlichtingen-diensten
Overheidssurveillance
Kennis van overheids-surveillance
Niet goed op de hoogte van de praktijk
Uit eigen onderzoek
Uit ervaringen van collega's
Via de media
Vermoedens van overheidssurveillance
Door bronnen die mogelijk doelwit waren
Geen vertrouwen in de integriteit van de overheid
Gekraak op de lijn
Uit contact met opsporingsdiensten
Uit waarschuwingen van bronnen/ collega's
Werk zou eventueel interessant kunnen zijn voor inlichtingen-diensten
Geen directe ervaring met overheids-surveillance
Enig vertrouwen in de integriteit van de overheid
Geen signalen dat journalist zelf doelwit was
Journalisten kunnen niet weten of ze doelwit zijn
Niet interessant genoeg voor inlichtingen-diensten
Omvang surveillance-praktjken wordt overdreven
Gevolgen van overheidssurveillance bij journalisten
Geen *chilling effect*
Verandering van werkwijze
Gevolgen van overheidssurveillance bij bronnen
Chilling effect
Geen *chilling effect*
Verzoek om andere werkwijze


Informatiebeveiligingstechnologie
Motieven voor het gebruiken van informatie-beveiligings-technologie
Beschermen veiligheid van bron
Geruststellen/ tegemoetkomen aan wens van bronnen
Belemmeringen voor het gebruiken van informatie-beveiligings-technologie
Bronnen niet afschrikken
Gebrek aan kennis/ervaring
Gebruiks-onvriendelijk
Nutteloos
Tijdrovend
Percepties van journalisten op het belang van informatie-beveiligings-technologie
Belang wordt nog onderschat
Belang wordt overschat
Genoeg bewustzijn in eigen werkomgeving
Eigen beveiliging zou beter kunnen
Journalisten in het algemeen moeten ermee kunnen omgaan
Mate van beveiliging is afhankelijk van het type onderzoek dat een journalist doet
Volledige bescherming tegen overheids-surveillance is onmogelijk
Bewustzijn in eigen werkomgeving kan beter
Strategieën voor het beveiligen van informatie
Adblocker
Analoge communicatie
Signal
Whatsapp
Beveiligde USB-sticks
Bewust bezig zijn met digitale sporen
Codetaal
Semafoon
Onvoorspelbaar zijn
Exclusieve platforms voor het delen van informatie
Wachtwoord-manager
Vermijden openbare sites
Vermijden van downloads
Vermijden openbare WiFi-netwerken
Protonmail/ versleuteld mailverkeer
Privacy Badger
PHP
Schone laptops
Telefoon uitzetten
Telegram
Theema
Firefox
Namen van bronnen niet in telefoon
Tor browser
Vermijden opslag in de cloud
VPN
Publeaks
Geen persoonlijke ervaring mee
Ervaring met bronnen van Publeaks
Redactie is aangesloten
Relatief weinig ervaring met informatie-beveiligings-technologie