RANDOMISED RESPONSE: over het hoe en waarom van privacybescherming

Randomised response is een methode voor het meten van sensitieve attitudes of gedrag, zoals wetsovertredingen, drugs- en alcoholgebruik en seksualiteit. In deze bijdrage geven we voorbeelden van randomised response en staan we stil bij de ethiek van de bescherming van privacy. We zullen laten zien dat het vanuit ethisch perspectief niet alleen belangrijk is dat randomised response de privacy beschermt, maar dat het evenzo essentieel is dat de respondenten de gehanteerde methode vertrouwen.

Ardo van den Hout & Marije Altorf

Randomised response is een statistische techniek om gegevens te verzamelen in een situatie waar respondenten terughoudend zijn in het geven van informatie (Warner 1965). De terughoudendheid kan verschillende redenen hebben. In sommige gevallen gaat het om overtredingen van de wet, bijvoorbeeld uitkeringsfraude of corruptie. Bij andere gaat het om privé-zaken zoals seksuele oriëntatie, abortus, gokverslaving.

Het basisidee van randomised response is dat er bescherming wordt geboden op individueel niveau, maar dat er desondanks statistische conclusies kunnen worden getrokken op het niveau van de groep die wordt onderzocht (de populatie). De veronderstelling is dat door de bescherming mensen eerder en beter zullen meewerken aan het onderzoek.

Randomised response met dobbelstenen

Er zijn verschillende technieken voor randomised response. We bespreken er een die illustratief is. Stel we willen wetsovertreding met betrekking tot een uitkering onderzoeken met de vraag 'Heeft u wel eens gefraudeerd ten aanzien van uw uitkering?'. Het is duidelijk dat dit een moeilijke vraag is om gegevens mee te verzamelen. Mensen die frauderen geven in het algemeen niet graag informatie over het niet volgen van de regels. Stel dat de vraag wordt gesteld aan een vrouwelijke respondent. Voordat ze ja of nee antwoordt, gooit ze met twee dobbelstenen. De uitkomst van de worp houdt ze voor zich. Als de uitkomst 2, 3 of 4 is, antwoordt ze met ja, ongeacht of ze wel of niet

heeft gefraudeerd. Als de uitkomst 5, 6, 7, 8, 9, of 10 is, antwoordt ze ja of nee naar waarheid. Als de uitkomst 11 of 12 is, antwoordt ze met nee, ongeacht of ze wel of niet heeft gefraudeerd.

Omdat de ondervrager de uitkomst van de worp niet kent, is het niet te achterhalen of een ja-antwoord daadwerkelijk correspondeert met fraude. Dit is de privacy-bescherming op individueel niveau. Echter, omdat we de kansverdeling van de uitkomst van de worp met de dobbelstenen kennen, kunnen we de kans berekenen dat fraudegedrag van een respondent leidt tot een ja-antwoord - mits de respondent de randomised response-instructies volgt. De volgende conditionele kansen kunnen worden afgeleid:

$$P(\text{ja}|\text{fraude}) = 33/36 \quad \text{en} \quad P(\text{ja}|\text{geen fraude}) = 6/36.$$

Vervolgens geldt:

$$\begin{aligned} P(\text{ja}) &= P(\text{ja}|\text{fraude})\,P(\text{fraude}) + P(\text{ja}|\text{geen fraude})\,P(\text{geen fraude}) \\ &= P(\text{ja}|\text{fraude})\,P(\text{fraude}) + P(\text{ja}|\text{geen fraude})\,(1-P(\text{fraude})) \end{aligned}$$

Waaruit volgt dat:

$$P(\text{fraude}) = \frac{P(\text{ja}) - P(\text{ja}|\text{geen fraude})}{P(\text{ja}|\text{fraude}) - P(\text{ja}|\text{geen fraude})}$$

De conditionele kansen in deze vergelijking zijn gegeven met kansverdeling van de uitkomst van de worp, de kans P(ja) kan worden geschat door de proportie ja-antwoorden in de steekproef. Aldus hebben we een schatting van P(fraude) en een statistische conclusie over het fraudegedrag in de populatie. Er is een formule voor de variantie van de schatter. De methode kan ook worden toegepast als er meer dan twee antwoordcategorieën zijn. Ook zijn er statistische modellen ontwikkeld waarmee het gedrag dat wordt onderzocht met randomised response kan worden verklaard aan de hand van variabelen zoals geslacht, leeftijd, of sociaal-economische status.

Statistisch gezien is het idee van randomised response dat data wordt verzameld met een techniek die misclassificatie toelaat. In het voorbeeld is P(ja| geen fraude) een misclassificatiekans, namelijk de kans dat een latent nee (geen fraude) wordt geobserveerd als een ja. Omdat het stochastisch gedrag van de misclassificatie bekend is, kan de statistische analyse hiervoor worden gecorrigeerd.

Als respondenten niet de randomised response-instructies volgen, heeft dit natuurlijk een ernstig effect op de data analyse. Wanneer het om een beperkte groep gaat die niet meewerkt door altijd nee te beantwoorden, dan is er statistisch nog wel iets te corrigeren (Böckenholt & Van der Heijden, 2007). In het algemeen echter ondergraaft het niet volgen van de instructies de data-analyse.

Post-randomisatie

Randomised response kan ook worden gebruikt om de privacy van respondenten te beschermen in een bestaand databestand. Dit heet post-randomisatie: misclassificatie wordt door middel van randomised response uitgevoerd nadat de gegevens zijn verzameld (Gouweleeuw et al., 1998). Post-randomisatie kan worden toegepast als de dataverzamelaar gegevens aan een derde partij wil doorgeven, dat wil zeggen aan onderzoekers die buiten de vertrouwensrelatie staan tussen de vragensteller en de respondent.

Stel dat het gaat om een bestand met gegevens over individuele spaartegoeden en dat naast het spaartegoed, ook een aantal persoonlijke gegevens wordt verzameld zoals leeftijdsgroep, geslacht, woonplaats en geboorteland. Als gegevens worden doorgegeven, dan worden directe indicatoren zoals naam en huisadres sowieso weggelaten, maar dat beschermt niet altijd afdoende. Als het gaat om een respondent in de leeftijdsgroep 70-80, die woont in Broek op Langendijk en geboren is in Peru, dan is het heel goed mogelijk dat deze combinatie van kenmerken uniek is in de steekproef én in de populatie. De identiteit van deze respondent is niet beschermd zonder extra maatregelen.

Het toepassen van post-randomisatie bestaat er uit dat voor bepaalde variabelen in het bestand geobserveerde waarden worden misgeclassificeerd en dat deze misclassificatie wordt uitgevoerd met conditi-

onele kansen die bekend zijn. Vervolgens wordt het bestand met de misgeclassificeerde gegevens vrijgegeven voor een derde partij tezamen met informatie over de conditionele kansen.

Verschillen tussen randomised response en post-randomisatie

Het grote verschil tussen randomised response en post-randomisatie is natuurlijk dat bij de eerste misclassificatie wordt uitgevoerd door de respondent zelf en bij de tweede de misclassificatie wordt uitgevoerd door een computer. Een ander verschil is dat randomised response typisch wordt toegepast op variabelen met latente waarden (bijvoorbeeld fraudegedrag) en post-randomisatie op variabelen met manifeste waarden (bijvoorbeeld geslacht, leeftijdsgroep). Een interessant verschil vanuit een statistisch oogpunt is dat bij post-randomisatie de misclassificatie-parameters kunnen worden bepaald aan de hand van de (al verzamelde) gegevens. Als er een maat is voor de bescherming, dan kan de misclassificatie daar op worden afgesteld (Van den Hout & Elamir, 2006). Bij randomised response is dit niet mogelijk omdat de misclassificatie-parameters moeten worden vastgesteld voordat de gegevens worden verzameld.

Het belang van privacy-bescherming: de scheiding tussen privé en publiek

Hoewel randomised response is ontworpen om in bepaalde situaties statistische resultaten te verbeteren, dringen zich ook ethische vragen op. We zullen deze bespreken aan de hand van het begrip privacy.

Als recht speelt privacy een belangrijke rol in de relatie tussen burgers en overheid, tussen burgers en bedrijven, alsmede tussen burgers onderling. In dit verband wordt privacy begrepen als controle over informatie over jezelf. Het lijkt niet meer dan vanzelfsprekend dat gegevens over godsdienst, politieke gezindheid of seksuele voorkeur niet zomaar worden doorgegeven aan een derde partij (zie ook de Wet Bescherming Persoonsgegevens <www.rijksoverheid.nl/onderwerpen/persoonsgegevens>).

Deze vanzelfsprekendheid suggereert een ethisch voorschrift: privacy moet worden beschermd. De redenen hiervoor zijn sterk verbonden aan een besef van wat het is om mens te zijn en deel te nemen aan de maatschappij. Privacy wordt fundamenteel geacht voor een open en vrije samenleving. Voor de Duits-Amerikaanse filosofe Hannah Arendt is deze eis zo wezenlijk dat ze geen enkele rol ziet voor de overheid in het privé-leven. Zij stelt hierbij de open samenleving recht tegenover de totalitaire samenleving, waar de overheid de huiskamer binnendringt door bijvoorbeeld kinderen tot klikken over hun ouders aan te zetten.

De positie van Arendt is sterk bekritiseerd vanuit verschillende perspectieven. Bowring (2011) geeft hiervan een goed overzicht. Arendts strenge tegenstelling tussen privé en publiek beschrijft ook niet de werkelijkheid van de Nederlandse samenleving. De overheid heeft toegang tot ons privé-leven, bijvoorbeeld in de vorm van regelgeving voor een paspoort, of voorwaarden voor een uitkering. Maar de tegenstelling helpt bij het nadenken over privacy en kan dienen als een waarschuwing voor wat mis kan gaan.

Privacy wordt niet alleen gezien als van belang voor de open samenleving, maar ook voor de ontwikkeling van het individu. Relaties tussen individuen kunnen zich alleen ontwikkelen wanneer de privé-sfeer niet wordt binnengedrongen of bekeken. Evenzo zijn spontaniteit, autonomie, creativiteit en persoonlijke verantwoordelijkheid gebaat bij de bescherming van privacy en bij het besef van deze bescherming. Dit laatste aspect doet een extra beroep op de onderzoeker. Bij statistisch onderzoek naar gevoelige zaken gaat het er niet alleen om te voorkomen dat informatie wordt verspreid. De onderzoeker moet ook voorkomen dat de deelnemer dit zal vrezen. Privacy is in deze context sterk verbonden met gemoedsrust (*peace of mind*).

De bescherming die randomised response en post-randomisatie geven betreft beide aspecten. Allereerst

wordt geprobeerd te voorkomen dat individuele informatie wordt verspreid. Die wordt onbekend gehouden (randomised response) of verdoezeld (post-randomisatie). Daarnaast moet de respondent beseffen dat privacy is gewaarborgd. Bij randomised response kan dit worden bewerkstelligd door actieve meewerking van de respondent.

Privacy lijkt zo beschermd bij het verzamelen van de gegevens. Maar dat is niet het hele verhaal. Gegevens van een randomised response-onderzoek kunnen leiden tot maatregelen die toch in het privéleven van de respondent ingrijpen. Dit is in het bijzonder het geval bij wetsovertredingen, waar inzichten verkregen met randomised response kunnen worden gebruikt om de controle op regelnaleving te veranderen. In dit geval zijn wel de individuele gegevens van de respondenten beschermd, maar medewerking aan het onderzoek kan nadelig uitwerken voor de groep en dus uiteindelijk ook voor de respondent.

Bij privé-zaken kan het evenzo zijn dat inzichten verkregen met randomised response worden gebruikt om veranderingen door te voeren. Maar deze veranderingen kunnen voordelig zijn voor de groep. Informatie over latente gokverslaving bijvoorbeeld, kan leiden tot een uitbreiding van zorgverlening. Dit is een optimale situatie voor het toepassen van randomised response. Dit voorbeeld maakt ook duidelijk dat er goede redenen zijn om niet aan Arendts strenge onderscheid tussen publiek en privé vast te houden. In deze laatste situatie is een beroep op de respondenten om mee te werken soms mogelijk. Als het onderzoek zaken betreft, waar privé-leven publiek kan worden bij ernstige gevallen (bijvoorbeeld faillissement bij gokverslaving), dan kunnen resultaten van het onderzoek leiden tot maatregelen die het aantal ernstige gevallen beperken en daarmee een betere scheiding bewerkstelligen tussen privé en publiek.

Conclusie

Randomised response biedt bescherming op het niveau van de respondent, maar niet op het niveau van de groep (de populatie). Voor de statistische analyse is het van uiterst belang dat de respondenten het randomised response-design volgen. Vanuit ethisch perspectief is het minstens even belangrijk dat onderzoek de privacy waarborgt. Informatie mag niet verder worden doorgegeven en respondenten moeten de methode hierin kunnen vertrouwen.

Deze ethische overwegingen geven tot slot inzicht in het functioneren van randomised response en post-randomisatie. Randomised response zal meer moeilijkheden opleveren wanneer medewerking van respondenten kan leiden tot maatregelen die op groepsniveau nadelig zijn. De optimale situatie voor randomised response is die waar respondenten beseffen dat hun privé-leven is beschermd en bovendien inzien dat het onderzoek kan leiden tot maatregelen die voordelig zijn voor hun groep en dus uiteindelijk misschien ook voor hen.

Literatuur

Arendt, H. (1998). *The Human Condition*. Chicago: University of Chicago Press.

Bowring, F. (2011). *Hannah Arendt: A Critical Introduction*. Londen: PlutoPress.

Böckenholt, U. & Van der Heijden, P. G. M. (2007). Item randomized-response models for measuring non-compliance: risk-return perceptions, social influences and self-protective responses. *Psychometrika*, 72, 245–262.

Gouweleeuw, J. M., Kooiman, P., Willenborg, L. C. R. J. & De Wolf, P.-P. (1998). Post randomisation for statistical disclosure control: theory and implementation. *Journal of Official Statistics*, 14, 463–478.

Van den Hout, A. & Elamir, E. A. H. (2006). Statistical disclosure control using post randomisation: Variants and Measures for Disclosure Risk. *Journal of Official Statistics*, 20, 711–731.

Warner, S. L. (1965). Randomized response: a survey technique for eliminating answer bias. *Journal of the American Statistical Association*, 60, 63–69.

Ardo van den Hout is wiskundige en werkt als docent-onderzoeker in het Department of Statistical Science, University College London.
E-mail: <ardo.vandenhout@ucl.ac.uk>

Marije Altorf is filosoof en werkt als docent-onderzoeker in de School of Theology, Philosophy, and History, St Mary's University College, London.
E-mail: <marije.altorf@smuc.ac.uk>