Aankondiging

Oratie
donderdag 24 maart 2022

Professor Wolter Pieters
hoogleraar aan de Radboud Universiteit / Faculteit der Sociale Wetenschappen met de leeropdracht *Work, Organisations & Digital Technology* zal op **donderdag 24 maart 2022 om 15.45 uur** precies zijn ambt aanvaarden, met het uitspreken van de rede getiteld:

Hacken op het werk: technologie, gedrag en veiligheid

De academische zitting vindt plaats in de Aula van de Radboud Universiteit in Nijmegen.

Vanwege coronamaatregelen kunnen helaas niet alle belangstellenden persoonlijk worden uitgenodigd om aanwezig te zijn.

De rede kan rechtstreeks worden gevolgd via een **livestream**:
www.ru.nl/aula/livestream

Het wordt zeker op prijs gesteld als u de rede online zou bijwonen.

Contactgegevens
Aula Radboud Universiteit
Bureau van de Pedel
pedel@co.ru.nl
Telefoon (024) 361 61 36
www.ru.nl/aula

Radboud Universiteit

IN DEI NOMINE FELICITER

Hacken op het werk: Technologie, gedrag en veiligheid

Wolter Pieters, inaugurele rede 24 maart 2022

Mijnheer de rector magnificus, zeer gewaardeerde toehoorders in de zaal en online,

Digitale technologie als smeermiddel

Crisissituaties zijn vaak de aanleiding voor niet-standaard praktijken op het werk. Toen wij als maatschappij werden geconfronteerd met de coronacrisis gingen we opeens voor een groot deel thuis werken. Het viel misschien in alle chaos niet zo op, maar *dat* deel van het crisismanagement ging eigenlijk nog best makkelijk. Want we hebben laptops, we kunnen verbinding maken met het bedrijfsnetwerk, en de rest gaat eigenlijk vanzelf. Ons werk is al compleet verweven met digitale technologie en het Internet, en dit kan er dan ook nog wel bij. Het verlies zat vooral in het werk als sociale omgeving.

Hoe relatief simpel deze overgang ook leek te zijn, de relaties tussen werk en digitale technologie zijn zeer complex geworden. Digitale technologie heeft voor velen van ons de werkomgeving en de daarbij behorende praktijken in de afgelopen decennia op zijn kop gezet. Vervelende administratieve klusjes, creatieve ontwerpprocessen, en politieke campagnes zien er allemaal compleet anders uit dan voor de digitale revolutie. En we merken het ook als wij willen werken, maar de technologie niet *werkt*. Dan kunnen we niet veel doen. Aan de TU Delft werkten zelfs de koffieapparaten niet als het Internet platlag. En toen de Universiteit van Maastricht slachtoffer werd van een aanval met gijzelsoftware moesten medewerkers zeer creatief zijn met alternatieve digitale technologieën om toch te kunnen blijven communiceren en het onderwijs en onderzoek draaiende te houden.

De verleiding is groot om technologie te zien als een middel om dingen makkelijker te maken; om ons werk uit handen te nemen. Digitale technologie maakt het eenvoudiger om producten te ontwerpen, documenten op te stellen, berekeningen uit te voeren, en deze zaken met anderen te delen. Het is een smeermiddel om allerlei processen soepeler te laten lopen. Deze instrumentele visie op technologie benadrukt de doel-middel relatie, en het dienende karakter van de technieken die we maken. Wat hier ontbreekt is dat technologie altijd ook neveneffecten met zich meebrengt. Techniek verandert de omgeving, het gedrag van mensen, en sociale relaties, en gezien alle berichten over administratieve fouten, cyberaanvallen, en fake news zijn die veranderingen niet altijd positief. Dat geldt ook voor de veranderingen in onze werkomgeving. De worsteling met de eindeloze stroom aan videomeetings in de afgelopen periode toont aan dat digitalisering soms ook verschraling met zich meebrengt, en dat niet iedereen even goed overweg kan met de nieuwe werkvormen.

Mijn leeropdracht gaat over werk, organisaties en digitale technologie. Ik doe dus onderzoek naar hoe digitale technologie in werkomgevingen gebruikt wordt, wat daar de redenen voor zijn, en wat de gevolgen zijn. Vanuit de gedragswetenschappen staat daarbij gedrag op het werk centraal, maar wel duidelijk in relatie tot de technische omgeving en de organisatie van het bedrijf. Ik zal in deze

rede eerst het landschap schetsen rond de impact van digitale technologie op werk. Daarna licht ik toe waar ik me in mijn onderzoek en onderwijs op wil concentreren.

Om uit te leggen hoe digitale technologie het werk veranderd heeft wil ik er drie zaken uitlichten. Allereerst de verandering van de eisen die aan het werk gesteld worden. Ten tweede nieuwe dreigingen in de werkomgeving door digitalisering. En ten derde de praktijken waarmee werknemers proberen het hoofd te bieden aan de complexiteit die de nieuwe eisen en dreigingen met zich meebrengen. Vaak is onofficieel gebruik van technologie onderdeel van deze praktijken, wat ik hier zal duiden als een vorm van *hacken*. Als laatste ga ik dan in op wat we kunnen doen om dit in goede banen te leiden.

Eisen

Allereerst wil ik het hebben over de eisen die aan werk gesteld worden. Als technologie bestaande praktijken makkelijker maakt, zou je denken dat dan ook de eisen minder hoog worden. Daarbij wordt vaak gesuggereerd dat bepaalde vormen van arbeid overbodig worden. Maar wat gemakkelijk vergeten wordt is dat met de technologische vernieuwing ook de bijbehorende normen gaan verschuiven, en dat de aan de resultaten gestelde eisen hoger worden. Stofzuigers maakten het huishouden makkelijker, maar zorgden ook voor hogere hygiënenormen, en dus meer werk. Robots kunnen bepaalde zorgtaken overnemen, maar verhogen tegelijkertijd de normen voor zorgtaken waar robots *niet* goed in zijn.

Deze verschuiving van eisen zien we ook terug in communicatie op het werk. Bijvoorbeeld eisen aan wanneer werknemers beschikbaar zijn om e-mails of andersoortige berichten te beantwoorden. Daardoor is de relatie tussen werk en privé onder druk komen te staan. Dit pakt voor iedereen anders uit; sommigen kunnen hier prima mee omgaan; voor anderen wordt het een chaos. Verschillende mensen hebben verschillende voorkeuren over de mate waarin aspecten van het leven door elkaar lopen, en hoe het werk ingericht wordt kan dus bepaalde groepen bevoordelen of benadelen.

Met digitale technologie kan er ook gemakkelijk meer geadministreerd worden. De verleiding is dan groot om ook te eisen *dat* er meer geadministreerd wordt, vanwege *accountability*. Verschillende beroepsgroepen zoals de zorg klagen over de toegenomen administratieve druk, waardoor de primaire processen in het gedrang komen. Digitalisering en bureaucratie lijken soms hand in hand te gaan, en elkaar te versterken. Daarbij verschuiven ook verantwoordelijkheden binnen organisaties. De eisen worden hoger, en bovendien ontstaan er conflicterende eisen, zogenoemde *differential pressures*, bijvoorbeeld wanneer iets snel *en* veilig moet. Daardoor kunnen werknemers het gevoel krijgen dat aan alle eisen voldoen onmogelijk is, en dus hun eigen keuzes gaan maken in wat wel en wat niet. Dat kan dan weer gevolgen hebben voor veiligheid van werknemers of patiënten, als de administratie van bijvoorbeeld medicatie niet klopt met de werkelijkheid.

Waar digitale technologie een belangrijke rol vervult als *resource* om het werk gedaan te krijgen, worden dus ook de *demands* hoger. Dit zien we ook terug in de *gig economy*, waar de eisen vrijwel geheel gedreven worden door de technologie. Bezorgers en taxichauffeurs krijgen opdrachten via de app, en moeten zichzelf in bescherming nemen als de eisen onverhoopt te hoog worden.

Digitale technologie is dus niet alleen een smeermiddel om werk makkelijker te maken, maar verandert ook de eisen die aan dat werk gesteld worden. Niet voor iedereen pakt die verandering goed uit, en het vereist soms creativiteit om aan alle gestelde eisen het hoofd te bieden.

Dreigingen

Hogere eisen kunnen dus ongewenste gevolgen hebben, maar dit is niet de enige dreiging die digitalisering met zich meebrengt. Dreigingen zijn dan ook de tweede belangrijke verandering. Door de afhankelijkheid van digitale technologie merken we het extra hard als er eens een keer iets niet *werkt*. Net als mensen die werken verrichten computers taken in opdracht, en net als bij mensen komt daar niet altijd uit wat je zou verwachten. Soms doet de computer het helemaal niet; soms is er een *bug* waardoor je in plaats van de verwachte bestelling slechts een foutmelding te zien krijgt, bijvoorbeeld door een mislukte software-update. En soms werkt het allemaal op zich wel, maar werkt het *in de praktijk* niet. Er is dan geen goede match tussen wat het systeem kan en wat de medewerkers nodig hebben om hun taken te verrichten. Vaak worden gefaalde IT-projecten bij de overheid aangehaald om dit te illustreren.

Maar in cyberspace gaan dingen niet alleen per ongeluk mis. We hebben inmiddels te maken met wereldwijd opererende cybercriminelen, die digitale zwakheden aangrijpen om zich toegang te verschaffen tot systemen. Dat kan betekenen dat er informatie wordt gestolen, maar ook dat systemen gegijzeld worden totdat er losgeld betaald is. Alhoewel softwarefouten nog steeds een cruciale rol spelen bij cyberaanvallen heeft ook gedrag belangrijke invloed, en daar gaat psychologie achter schuil. Denk dan bijvoorbeeld aan het klikken op links in phishing e-mails. Maar ook de experimenten die we aan de Universiteit Twente hebben gedaan met trucs om mensen sleutels of laptops afhandig te maken laten dit overtuigend zien: veel mensen geven met een goede smoes van alles af.

Waar cyberaanvallen soms uit zijn op specifieke kennis van bedrijven of overheden gaat het ook vaak om persoonsgegevens, zoals creditcardnummers. Met de komst van privacywetgeving zijn bedrijven zich meer bewust geworden van de persoonsgegevens die ze verwerken en de bescherming die daarbij hoort. Maar de praktijk is hardnekkig. Er wordt nog steeds te veel data gedeeld, data staat op te veel plekken, gegevens worden niet verwijderd als ze niet meer nodig zijn, en beveiligde omgevingen zijn er wel maar worden niet altijd juist gebruikt. Zo kreeg ik van een verzekeraar via een beveiligde omgeving een leeg formulier, met het verzoek om het ingevulde formulier – met gevoelige gegevens – per e-mail terug te sturen. Zo moet het dus niet.

Daarbij moet opgemerkt worden dat de nadruk in het debat over digitalisering wel erg op privacy is komen te liggen. Dat heb ik eerder vanuit de filosofie onderzocht, met de boodschap om meer te kijken naar het effect op de maatschappij als geheel in plaats van het effect op de privacy van individuen. Terecht heeft iHub, het interdisciplinaire platform van de Radboud Universiteit over digitalisering en samenleving, ook bijvoorbeeld solidariteit, expertise en vrijheid op de agenda staan als waarden waar digitalisering invloed op heeft. Ook de mechanismen om privacy te beschermen, sterk gericht op toestemming van het individu, zijn vanuit de psychologie problematisch, omdat er te vaak te veel gevraagd wordt. De meeste mensen klikken de toestemmingsverklaringen voor cookies klakkeloos weg. Bovendien wordt instemmen vaak makkelijk gemaakt, terwijl je veel moeite moet doen om bepaalde data *niet* te delen. Maar als we het rond privacy al niet eens in orde krijgen, hoe moet het dan met die andere waarden?

De afhankelijkheid van digitale technologie, de complexiteit rond onder andere privacy en daarbij behorende fouten, en de toenemende cybercriminaliteit bedreigen dus de mogelijkheden van werknemers om aan de eisen van het werk te voldoen.

Praktijken

De hogere eisen en toegenomen dreigingen hebben ook gevolgen voor de praktijken op het werk, de derde belangrijke verandering. Eisen en dreigingen leggen extra druk op het functioneren van medewerkers in een gedigitaliseerde omgeving. Bestaande manieren van werken voldoen vaak niet meer, maar kennis van alternatieven is niet altijd aanwezig, of de overstap wordt als te ingewikkeld gezien.

Tegelijkertijd wordt er juist ook *wel* naar alternatieven gezocht. Als de bedrijfs-ICT te ingewikkeld is of te veel beperkingen heeft gaan medewerkers op zoek naar eigen oplossingen waar de organisatie helemaal geen controle over heeft, zoals privé-mail, WhatsApp, en Dropbox. Deze zogenaamde "schaduwtechnologie" voldoet vaak niet aan eisen rond privacy, en is ook niet altijd voldoende beveiligd. Medewerkers proberen soms wel hun eigen "schaduwveiligheid" te organiseren, maar omdat hun ideeën over hoe de technologie werkt niet altijd overeenkomen met die van de experts is dat zeker niet altijd waterdicht.

Ook op andere gebieden zien we deze "workarounds" in organisaties. Dit is een vorm van "hacken" in brede zin, namelijk het gebruik van technologie op manieren waar deze niet voor bedoeld was. Deze "omheenwerkingen" laten vaak de spanning zien tussen de primaire processen rond productiviteit en de andere waarden die ook aandacht vragen in de organisatie. Waar ooit dingen op een bepaalde manier georganiseerd waren voor bijvoorbeeld veiligheid, wordt dit vaak vergeten (of zelfs bewust genegeerd) als het de productiviteit in de weg zit. Zo was bijvoorbeeld een gat in de gasleiding naar ons huis dichtgeplakt met ducttape. En bij het kabelbaanongeluk in Italië vorig jaar was de noodrem uitgeschakeld omdat deze voor vertragingen zorgde. In dit soort situaties worden tijdelijke oplossingen vaak permanent. Het is dus cruciaal dat organisaties zicht hebben op de hacks, en waar nodig de praktijken opnieuw in balans brengen met de te beschermen waarden.

Dit betekent ook dat signalen van problemen op tijd moeten worden opgepikt. In veel gevallen kunnen er dingen worden opgemerkt voordat het echt ergens mis gaat. Maar afwijkingen die vaker voorkomen worden in toenemende mate als normaal gezien, en men realiseert zich niet dat er een achterliggend probleem is. Bij de grote explosie bij Shell Moerdijk in 2014 werden fluctuaties in druk en temperatuur bijvoorbeeld niet als bedreigend gezien. En bij de cyberaanval op de Universiteit van Maastricht werd wekenlang niet opgemerkt dat de aanvaller actief was op het netwerk. Ook in de coronacrisis verschoven normen: mensen droegen op de universiteit wel een mondkapje wanneer dat verplicht was, maar de looproutes volgen was te veel gedoe. Hoe voorkomen we dan normalisering van afwijkingen? En hoe zit dat met bijvoorbeeld signalen van pesten of grensoverschrijdend gedrag op het werk, of wetenschappelijke fraude?

Er zijn dus allerlei manieren om met de combinatie van eisen en dreigingen in een werkomgeving om te gaan. Maar als dat in de werkpraktijken niet op een goede manier gestuurd wordt ontstaan vaak risico's voor bijvoorbeeld veiligheid. Het is erg gemakkelijk om te denken "dat overkomt ons niet", zeker als er druk op de ketel zit om een product snel op de markt te brengen of het werk van uitgevallen collega's er even bij te doen.

Interventies

Wat zouden organisaties dan moeten doen om de effecten van digitalisering op de werkvloer zodanig te sturen dat waarden zoals veiligheid en privacy voldoende beschermd worden? Veel initiatieven

rond *awareness* richten zich te eenzijdig op kennisoverdracht. En dat heeft slechts een beperkt en vaak kortdurend effect op gedrag. Wat moeten we dan wel?

Voor zover we toch inzetten op kennisoverdracht moet er in ieder geval goed nagedacht worden over de vorm en de inhoud van de boodschap. De *framing* van de risico's, het gewenste gedrag en de effecten daarvan speelt een belangrijke rol in de gedragsverandering. Zo is het rond veiligheid cruciaal of de boodschap wordt verpakt als het voorkomen van ongelukken (verlies) of het bijdragen aan een veilige omgeving (winst). Mensen bang proberen te maken of schaamte te laten voelen kan in sommige situaties helpen, maar kan ook averechts werken.

Waarden benadrukken kan daarnaast onder andere met *priming*: als mensen recent iets over veiligheid gehoord hebben, of iets gedaan hebben dat in het teken staat van veiligheid, zijn ze eerder geneigd het mee te nemen in hun afwegingen. Dat is waarom sommige bedrijven het vasthouden van de trapleuning zo benadrukken. We willen een *klimaat* creëren in de organisatie waarin veiligheid een belangrijke rol speelt, en mensen elkaar durven aan te spreken, en het durven te signaleren als ze iets zien waarvan ze denken dat het riskant is. Dan kan het bijvoorbeeld gaan om workarounds die onveilig zijn. Daar hoort bij dat er regelmatig over veiligheid gesproken wordt, al was het maar om dit in focus te houden.

Tenslotte moeten we ook kijken naar de technologie zelf. Een voorbeeld daarvan is het op tijd verwijderen van gevoelige bestanden, zoals informatie over sollicitaties. Als je verwacht dat medewerkers zelf het initiatief nemen voor het verwijderen kom je misschien bedrogen uit, want het heeft nooit echt prioriteit. Dat moet je dus anders organiseren, bijvoorbeeld door data een einddatum mee te geven. En als je wilt dat mensen minder snel in phishing e-mails trappen, moet je misschien een afkoelperiode instellen voor links en attachments nadat mensen de e-mail geopend hebben. Dat wil zeggen: mensen worden gedwongen om even te wachten voordat ze actie kunnen ondernemen, en denken dan hopelijk iets beter na. Maar we moeten daarbij wel voorkomen dat mensen er last van hebben en daarom hun privé-mail gaan gebruiken. Veilig gedrag moet ook makkelijk zijn.

Er zijn dus allerlei manieren om binnen de eisen en dreigingen in de werkomgeving digitaal gedrag te proberen te sturen. De centrale vraag daarbij is hoe we kunnen zorgen dat belangrijke waarden zoals veiligheid voldoende worden meegewogen in beslissingen op het werk, zowel bij de keuze voor technologie als het gebruik ervan. Maar het is cruciaal dat die interventies zelf niet alleen maar de eisen *nog* hoger maken, want dan wordt het probleem niet opgelost.

Onderzoek

Mijn achtergrond ligt niet in de sociale wetenschappen. Maar vanuit de informatica en de techniekfilosofie heb ik wel al veel meegekregen over de interactie tussen mensen en technologie. Vanuit de informatica werd duidelijk dat er heel veel verschillende vormen van interactie en samenwerking met computers mogelijk zijn. Vanuit de techniekfilosofie kwam het inzicht dat apparaten de manier veranderen waarop mensen de wereld waarnemen, en de manier waarop zij handelen. Dat betekent ook dat je door technologie anders te ontwerpen percepties en gedrag kunt beïnvloeden. Maar zowel de informatica als de techniekfilosofie zijn primair ontwerpende wetenschappen. De een ontwerpt mechanismen, de ander conceptuele kaders. Dat is toch iets anders dan daadwerkelijk de interactie tussen mensen en techniek empirisch bestuderen, en zo na te gaan wat technologie *in de praktijk* met gedrag doet. Als je een knop ergens anders op het scherm zet, klikken mensen misschien vaker of minder vaak.

Mijn belangstelling voor de sociale wetenschappen werd gewekt tijdens mijn promotie aan de bètafaculteit van de Radboud Universiteit. In mijn onderzoek naar de discussie over de veiligheid van digitaal stemmen bij verkiezingen bleek al snel hoe belangrijk communicatie en vertrouwen waren in de acceptatie van technologie. En ook mijn rol bij het vak Onderzoeksmethoden voor Informatiekunde droeg bij aan mijn interesse in de vraag hoe je goed sociaal-wetenschappelijk onderzoek opzet.

Na een intermezzo in de praktijk van het beleid ging ik me bezighouden met het managen van risico's rond cybersecurity. Hoe ondersteun je beslissingen over welke maatregelen een organisatie zou moeten nemen om cyberrisico's het hoofd te bieden? Daarbij werd al snel duidelijk dat het hier niet alleen gaat over het blokkeren van netwerkverkeer. Ook fysieke toegang tot gebouwen en onveilig gedrag kunnen bijdragen aan cyberaanvallen en datalekken. Ook hier vond ik de rol van de mens weer fascinerend. Vandaar dat ik, met als basis een aantal onderzoeken naar onveilig gedrag, besloot ook echt de sociaal-wetenschappelijke kant op te gaan, met de interdisciplinaire bagage aan boord.

Interventies laten duidelijk de interacties zien tussen ontwerpende wetenschap en beschrijvende wetenschap. Aan de ene kant willen we weten hoe gedrag afhangt van de omgeving. Aan de andere kant kan juist het anders ontwerpen van die omgeving mogelijk bijdragen aan veiliger gedrag. Dit soort onderzoek grijpt op verschillende manieren in elkaar: beschrijvend onderzoek naar de rol van de omgeving kan inspiratie bieden voor *design science* voor interventies, en het effect van die interventies kan dan weer met beschrijvend onderzoek getoetst worden.

Wat is dan de meerwaarde van dit interdisciplinaire perspectief? Ik licht er drie thema's uit.

1. Waarschuwingssignalen

Het eerste thema is hoe werknemers en organisaties omgaan met waarschuwingssignalen op het werk, en hoe de respons effectiever kan worden ingericht. Veiligheid in organisaties, ook digitale veiligheid, is onlosmakelijk verbonden met waarschuwingen. Ik heb al genoemd dat veel ongelukken en cyberincidenten gebeurden ondanks signalen dat er iets niet in orde was. Waarom reageren mensen dan niet adequaat op waarschuwingen? Daar kunnen allerlei redenen voor zijn. Men denkt dat het allemaal wel meevalt. Dat er nog wel even afgewacht kan worden of het probleem zich misschien vanzelf oplost. Of men is bang om op het matje geroepen te worden als het vals alarm is. Door de omgeving te veranderen kan ook het gedrag beïnvloed worden, bijvoorbeeld door het rapporteren van problemen zoals phishing e-mails makkelijker te maken in de technologie, maar ook door de perceptie van de gevolgen van een vals alarm te reduceren door werknemers op een andere manier op fouten aan te spreken.

In eerste instantie ga ik samen met de TU Delft onderzoek doen naar hoe operators van elektriciteitsinfrastructuur omgaan met waarschuwingen van mogelijke cyberdreigingen in de control room. Daar staat duidelijk de relatie tussen mens en techniek op de voorgrond, en is kennis van die interactie vanuit verschillende disciplines cruciaal om het gedrag van operators te begrijpen. Maar het onderwerp van waarschuwingssignalen op het werk is veel breder. We gaan samen met sociale psychologie ook kijken naar signalen rond sociale veiligheid, bijvoorbeeld rond grensoverschrijdend gedrag. Hoe kun je als organisatie zorgen dat medewerkers signalen durven af te geven, en er adequaat op zulke signalen wordt gereageerd?

2. Digitale technologie en verantwoordelijkheid in organisaties

Het tweede thema is de relatie tussen digitale technologie en verantwoordelijkheid in organisaties. Ik wil onderzoeken hoe digitale technologie de percepties van en het omgaan met verantwoordelijkheid in organisaties verandert.

De ondersteuning van beslissingen door digitale technologie wordt met de opkomst van kunstmatige intelligentie steeds geavanceerder. Maar wat is de motivatie van een werknemer om in haar beslissing af te wijken van een door zo'n systeem gegeven advies? Dat betekent namelijk dat zij aangesproken kan worden op de gevolgen als het een verkeerde beslissing blijkt te zijn. Als het advies van het systeem gevolgd wordt kan er altijd naar de technologie gewezen worden als de bron van de ellende. Ik wil onderzoeken wat er precies gebeurt als mensen eigenlijk tegen een advies van een computer in zouden moeten gaan, maar het vanwege de mogelijke consequenties misschien toch niet doen. Maar ook wat er gebeurt als ze er juist wèl tegenin gaan.

Ook de selectie van technologie voor gebruik op het werk roept vragen rond verantwoordelijkheid op, met name als die technologie impact heeft op privacy. Onder welke voorwaarde kunnen organisaties bijvoorbeeld software uitrollen die data van medewerkers aan derden ter beschikking stelt? En hoe ervaren medewerkers dat? Maar ook de keuzes die medewerkers zelf maken rond technologiegebruik zijn verweven met verantwoordelijkheid. Ik wil begrijpen hoe werknemers nadenken over hun verantwoordelijkheid als ze schaduwtechnologie gebruiken die niet door de organisatie wordt ondersteund. Samen met iHub gaan we kijken naar hoe scholen, docenten en studenten technologie selecteren voor het onderwijsproces, en hoe belangrijke waarden daarin kunnen worden meegenomen.

Dan is er nog het werken op afstand, waar digitale technologie uiteraard een cruciale rol in speelt. Ook in een weer normalere situatie zullen veel werknemers deels thuis blijven werken. Wie is er dan op welke manier verantwoordelijk voor de inrichting van de werkplek, de sociale cohesie in het team, en de kwaliteit van het werk? En hoe zorgen we dat ook op afstand belangrijke waarden worden meegenomen in beslissingen? Het PhD-project van Wieke Knol zal zich concentreren op gedrag en verantwoordelijkheid van leidinggevenden bij hybride werken.

3. Workarounds

Als derde wil ik inzetten op onderzoek naar de genoemde "omheenwerkingen", de workarounds, shortcuts en hacks op de werkvloer. Als procedures of technologie in de weg zitten van efficiëntie, hoe gaan werknemers daar dan mee om? Ik wil onderzoeken wie er onder welke omstandigheden aan workarounds doet, en hoe organisaties kunnen zorgen dat werknemers hun werk kunnen doen, en tegelijkertijd waarden zoals veiligheid waarborgen.

Als basis dient mijn bestaande onderzoek naar keuzemodellering. We hebben aan de TU Delft rond de aanschaf van slimme apparaten laten zien dat mensen cyberveiligheid en privacy best willen meewegen, maar het niet spontaan als criterium noemen. Met keuzemodellering kunnen we systematisch in kaart brengen hoe zwaar mensen waarden laten meewegen bij zulke keuzes. En we kunnen laten zien hoe priming en framing dit beïnvloeden.

Waarschuwingssignalen, verantwoordelijkheid en workarounds vormen dus de kern van mijn onderzoeksagenda. Ik wil daarbij uitdrukkelijk niet de techneut zijn in een wereld van sociale wetenschappen, maar vooral laten zien hoe ontwerpende wetenschappen - conceptueel, technisch, en communicatief - de gedragswetenschappen kunnen verrijken, en omgekeerd.

Onderwijs

Dat laatste idee zal ook een centrale rol spelen in mijn onderwijs. In het onderwijs zijn er twee thema's die ik verder wil ontwikkelen: cyberpsychologie en psychologie van de veiligheid, beide met name toegepast op de werkcontext. Bij cyberpsychologie gaat het om beslissingen *over* technologie (wat gebruik ik?) en beslissingen in het werken *met* technologie (hoe gebruik ik het?) Beide hangen samen met de mentale modellen die mensen van de werking van de technologie hebben, maar ook met de vormgeving van de technologie.

Bij psychologie van de veiligheid gaat het over de invloed van gedrag op veiligheid op de werkvloer, en de rol van de omgeving daarbij. Naast cultuur maakt ook technologie onderdeel uit van die omgeving, via bijvoorbeeld architectuur en interfaces. Het aandachtsgebied van workarounds koppelt cyberpsychologie en psychologie van de veiligheid: het gaat over technologiegebruik, maar ook over wat dat betekent voor veilig werken.

Ik ben er daarbij van overtuigd dat meer dialoog en discussie in het onderwijs van grote waarde kan zijn, ook tussen docenten onderling. De meest waardevolle momenten ontstaan bijvoorbeeld wanneer de coördinator van een vak in discussie gaat met een gastspreker. Maar ook interviewtechnieken kunnen hier helpen: studenten kunnen een gastdocent interviewen in plaats van naar een verhaal luisteren.

Ik vind het daarnaast belangrijk om onderwijs en onderzoek elkaar te laten versterken. Idealiter leveren opdrachten die studenten doen ook een bijdrage aan het beantwoorden van een onderzoeksvraag, bijvoorbeeld hoe keuzes voor digitale technologie of veiligheidsmaatregelen gemaakt worden in een casus.

Uiteraard heeft digitale technologie ook het onderwijs zelf flink veranderd, zowel voor als tijdens de coronacrisis. De digitale leeromgevingen zijn niet meer weg te denken, en ook hier geldt dat dit voor sommige studenten beter zal werken dan voor anderen. Ook hier is het zaak om goed te begrijpen hoe technologie en praktijken op elkaar afgestemd kunnen worden. Hoe gaan we bijvoorbeeld om met de beschikbaarheid van opnamen van colleges in relatie tot de meerwaarde van fysieke aanwezigheid voor interactie?

Het is daarnaast interessant om te zien hoe percepties van veiligheid zich manifesteren in het onderwijs. Zo mocht in de herfst van 2021 van de overheid vrijwel alles weer op de campus binnen beperkte groepsgroottes, maar voelden niet alle groepen studenten zich daar prettig bij. Dit legde dan weer verantwoordelijkheid bij de docenten, die breed gedragen oplossingen moesten zoeken in combinaties van live, online en hybride. Ook hier dus een interessante dynamiek rond veiligheidscultuur, en de rol van van buitenaf opgelegde normen.

Digitalisering in de academische wereld

Tot slot iets over de academische wereld. Ook daar heeft digitalisering uiteraard grote veranderingen met zich meegebracht. Hier wil ik de filosofe Hannah Arendt aanhalen, met haar *Vita activa* en het onderscheid tussen arbeid, werk en handelen. Arbeid komt voort uit noodzaak, werk creëert iets blijvends, en handelen gaat over het je in vrijheid en uniciteit kunnen uiten. De transformatie naar de *Vita digitala* heeft in de wetenschap impact gehad in alle drie domeinen, maar er liggen twee zaken in het bijzonder op de loer. Ten eerste de verantwoordingscultuur, mede mogelijk gemaakt door digitalisering, waarin de meetbare output van het *werk* meer centraal is komen te staan, terwijl de processen van verantwoording zelf tot meer *arbeid* leiden. Dit kan ten koste gaan van het in vrijheid

handelen. Ten tweede is het *handelen* van de wetenschapper zelf van binnenuit veranderd door de komst van sociale media, en daarmee andere manieren van uitwisseling van visies, en een andere rol van de wetenschapper daarbij. De ingewikkelde dynamiek van percepties, alternatieve werkelijkheden, en uiteindelijk gedrag maakt het moeilijk kennis op een integere en tegelijk effectieve manier te delen. Maar ook hier kunnen juist de gedragswetenschappen een bijdrage leveren aan oplossingen. De invloed van communicatie op gedrag in de coronacrisis heeft het belang hiervan nog eens benadrukt.

Omdat de universiteit ook zelf een organisatie is waar de impact van digitalisering groot is, wil ik ook de samenwerking opzoeken met de afdeling ICT voorzieningen van de Radboud Universiteit. Er liggen mogelijkheden rond de voorbeelden die ik genoemd heb voor gedragsverandering op het gebied van privacy en cybersecurity, en de invoering van nieuwe software. Ik zie daarbij verantwoordelijk gebruik van digitale technologie nadrukkelijk ook als onderdeel van de duurzaamheidsagenda van de Radboud Universiteit. Het gaat dan vooral om de vaak vergeten *sociale* duurzaamheid, en het daarbij horende beschermen van publieke waarden zoals privacy en transparantie.

Dankwoord

Dat brengt mij bij het dankwoord. Uiteraard bedank ik de afdeling, de faculteit en het College van Bestuur voor het vertrouwen. En in dit geval met een specifieke aanvulling. Het is niet vanzelfsprekend dat wetenschappers uit andere vakgebieden in aanmerking komen voor een positie als deze. Dat ik hier toch sta laat zien dat de Radboud Universiteit interdisciplinariteit en team science serieus neemt. Vooral daarom wil ik mijn waardering uitspreken.

Verder zijn er vele academici die mij in de afgelopen jaren op allerlei manieren hebben geholpen en geïnspireerd. Ik ga de namen niet allemaal noemen. Wel noem ik een aantal communities. Allereerst de docenten, studenten en alumni van de opleiding Wijsbegeerte van Wetenschap, Technologie en Samenleving van de Universiteit Twente. Als ik destijds na mijn eerste jaar informatica niet voor een combinatie met WWTS had gekozen waren dingen ongetwijfeld anders gelopen. De brede belangstelling en scherpe geest van de betrokkenen hebben mij geïnspireerd om ook verder te denken, en dat ook weer op een inspirerende manier op te schrijven.

Verder wil ik de New Security Paradigms Workshop noemen. De eerste keer dat ik deze workshop bezocht was in 2011. De centrale vraag is hoe we de veiligheid van digitale technologie verder kunnen brengen door van de gebaande paden af te gaan. Nieuwe ideeën vanuit onverwachte hoek zijn welkom, ieder paper krijgt een uur voor presentatie en discussie, en feedback is zeer constructief. Dat betekent ook wel dat er verwacht wordt dat je iets met de feedback doet. Ook dit is weer een community van mensen met een brede belangstelling en scherpe geest die mijn denken over digitale technologie mede vormgegeven heeft. Veel inspiratie kwam daarnaast ook uit de interdisciplinaire seminars in Schloss Dagstuhl en het Lorentz Center die ik bijgewoond en georganiseerd heb.

In het begin van mijn carrière was niet iedereen overtuigd van mijn interdisciplinaire aanpak. Schoenmaker blijf bij je leest, heb ik wel eens gehoord. Vooral in het begin van je carrière zou het niet verstandig zijn om verschillende *lenzen* te hanteren, omdat je toch vooral afgerekend wordt op heel goed zijn in heel weinig. Maar het bloed kruipt waar het niet gaan kan. Mijn fascinatie voor nieuwe perspectieven en verbindingen heeft het mogelijk gemaakt om de verschillende rollen te vervullen die ik de afgelopen jaren heb gehad, en heeft ook deze laatste stap weer mogelijk gemaakt. Daarom wil ik iedereen bedanken die de potentie van mijn interdisciplinaire onderzoeksagenda

gezien heeft, en mij gesteund heeft bij het verder ontwikkelen daarvan. En daar vallen veel mensen onder.

[Persoonlijk dankwoord vanwege privacy niet in deze versie.]

Ik heb gezegd.