

Dark Patterns in digitale gebruikersomgevingen

Robin Wacanno
11741163

Bij het gebruik van websites, mobiele applicaties en programma's op je computer bedien je deze met een door de ontwikkelaar ontworpen gebruikersomgeving. Deze ontwikkelaar, of in sommige gevallen de opdrachtgever, heeft er soms baat bij dat de gebruiker zicht binnen de betreffende gebruikersomgeving op een bepaalde manier gedraagt of bepaalde keuzes maakt. Ik zelf—en dat is ook de reden dat het voor mij een zorgelijke ontwikkeling begon te worden—ben dit dikwijls tegen gekomen bij het moeten accepteren van *cookies* voor een bepaalde website. Websites maken het vaak namelijk een stuk gemakkelijker om alles maar te accepteren, dan om als gebruiker kritisch te kijken naar de manier waarop deze *cookies* gebruikt gaan worden en of je dit wel wil. Dit fenomeen van gebruikersomgevingontwerp een *dark pattern* genoemd.

Bij *dark patterns* zijn verschillende categorieën te onderscheiden, zoals ook beschreven in Gray e.a. 2018. Allereerst is er het zogenaamde *nagging*. Hierbij worden een of meerdere acties van de gebruiker herhaaldelijk onderbroken door een verplichte interactie. Een voorbeeld hiervan is bijvoorbeeld een *pop-up* die verschijnt en door de gebruiker weg geklikt moet worden alvorens deze verder kan gaan met het gebruik van een website. Vervolgens is *obstruction*, wat—zoals de naam misschien al doet vermoeden—op de een of andere manier een gebruiker in de weg staat. Het doel is hierbij voorkomen dat een gebruiker een bepaalde handeling uitvoert. Een goed voorbeeld hiervan is het in de introductie genoemde accepteren van *cookies*. Mocht een gebruiker zelf de keuze willen maken bepaalde *cookies* te blokkeren, dan worden deze opties vaak verscholen achter meerdere menu's. Hierdoor is er een kans dat een gebruiker toch maar met de standaard—vaak meer op privacy inbreuk makende—instellingen akkoord gaat. *Sneaking* is ook een veelvoorkomend fenomeen, waarbij geprobeerd wordt bepaalde informatie voor de gebruiker verborgen te houden voor een gebruiker wanneer deze eigenlijk relevant is bij het maken van een keuze. In Gray e.a. 2018 wordt het voorbeeld genoemd van een website die gebruikers bij het uitschrijven voor een nieuwsbrief akkoord laat gaan met een overeenkomst die het bedrijf achter de website toestemming geeft om de gegevens van de betreffende gebruiker door te verkopen. De volgende categorie, *interface interference*, is ook iets wat bij het accepteren van *cookies* veel terug komt. Middels deze techniek wordt er op bepaalde keuzes door een specifieke opmaak meer nadruk gelegd. In het geval van een *cookie*-melding zou dit bijvoorbeeld gedaan kunnen worden door de knop die alle *cookies* accepteert groter te maken en een dui-

delijke kleur te geven, terwijl de knop met meer opties er gewoon uit ziet als niet-klinkbare tekst. De laatste categorie is *forced action* en spreekt voor zich; een gebruiker moet een bepaalde handeling uitvoeren alvorens zekere functionaliteit beschikbaar wordt gesteld. De meeste *dark patterns* die men in het echt tegen zal komen kunnen onder meerdere van de categorieën geschaard worden, maar dit zijn wel duidelijke patronen die veelvuldig voorkomen.

Het gebruik van *dark patterns* is in mijn optiek op meerdere manieren kwaadaardig. Een opzicht waarin het inbreuk maakt op onze menselijke waarde is door het tornen aan de menselijke autonomie (Royakkers e.a. 2018). Het is duidelijk dat het gebruik van *dark patterns* als hoofddoel heeft het sturen van de menselijke gedachtegang en het menselijke keuzeprocess. De meeste *dark patterns* spelen in op mechanismen in het onderbewustzijn (Bösch e.a. 2016) en zorgt er zo voor dat het niet de gebruiker zelf is die bijvoorbeeld akkoord gaat met het delen van informatie, maar dat deze door subtiele suggesties in de gebruikersomgeving gestuurd wordt een keuze te maken die misschien haaks op zijn belang. Ook geeft deze strategie blijk van een verstoorde machtsverhouding (Gray e.a. 2018; Royakkers e.a. 2018). In het geval van *forced action* kan de mens uitgesloten worden van het gebruik van bepaalde diensten als hij niet instemt met de eisen die een bedrijf achter een website of applicatie stelt. Mocht het gaan om een dienst die van groot belang is, denk bijvoorbeeld aan een systeem gebruikt in scholen of op een werkplek, dan heeft de gebruiker geen keus en zal hij met misschien voor hem onacceptabele voorwaarden akkoord moeten gaan.

Wanneer gekeken wordt naar *dark patterns* in de context van Instrumentalisme en technologisch determinisme, zoals beschreven in Becker 2015, is er een duidelijke scheiding te bespeuren. Aan de ene kant heb je zij die het als middel inzetten. Als bedrijf profiteer je er natuurlijk enorm van als je nog meer kostbare data van gebruikers kan buitmaken door een gebruikersomgeving zo aan te passen dat zij toestaan dat deze data verzameld wordt of dat gebruikers deze zelf prijs geven. In die zin zijn *dark patterns* voor een bedrijf in de eerste plaats duidelijk Instrumentalistisch.

Woorden: ###

Referenties

- [1] Marcellinus Jozef Becker. *Ethiek van de digitale media*. Boom, 2015.
- [2] Christoph Bösch e.a. “Tales from the dark side: Privacy dark strategies and privacy dark patterns”. In: *Proceedings on Privacy Enhancing Technologies* 2016.4 (2016), p. 237–254.
- [3] Colin M Gray e.a. “The Dark (Patterns) Side of UX Design”. In: *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM. 2018, p. 534.
- [4] Lambèr Royakkers e.a. “Societal and ethical issues of digitization”. In: *Ethics and Information Technology* 20.2 (jun 2018), p. 127–142. ISSN: 1572-8439. DOI: 10.1007/s10676-018-9452-x. URL: <https://doi.org/10.1007/s10676-018-9452-x>.