Jagoda Czerwiec

"Internet złych rzeczy", Julia Chmielecka, Bielsko-Biała 2017 : [recenzja]

Kultura Popularna nr 3 (57), 136-139

2018

Recenzja

DOI: 10.5604/01.3001.0012.7294

Julia Chmielecka *Internet złych rzeczy*, Bielsko-Biała, Pascal 2017

„Dopóki nie skorzystałem z internetu, nie wiedziałem, że na świecie jest tylu idiotów". To cytat, przypisywany Stanisławowi Lemowi, wpasowuje się w przekaz książki Julii Chmieleckiej, *Internet złych rzeczy*. W czasie, kiedy piszę tę recenzję, w całej Europie trwają dyskusje na temat RODO (Rozporządzenie o Ochronie Danych Osobowych). Jest to akt prawny, który powinien chronić naszą anonimowość. Czy jednak coś takiego jak anonimowość w ogóle istnieje? Czy rozsądni ludzie mogą w to wierzyć? Czy Stanisław Lem rzeczywiście aż tak trafnie opisał społeczność internetu?

Recenzowana książka ukazuje ciemną stronę internetu. Podczas przechodzenia przez takie rozdziały jak: *Po co nam anonimowość*, *Trollowanie*, *Cyberbulling* czy *Pedoporno*, poznajemy zakamarki dwóch stron tego medium, *clearnet* i *darknet*. Jak się jednak okazuje, strony te nie są aż tak różne, jak mogłoby się wydawać.

Użytemu wyżej rozróżnieniu poświęcony jest cały pierwszy rozdział. *Clearnet* to strony indeksowane – ogólnodostępne, możliwe do znalezienia przez wyszukiwarkę. Drugi typ natomiast obejmuje te, które związane są z nielegalną działalnością, dające teoretyczną anonimowość użytkownikom, wymagające wykorzystania specjalnego programu do łączenia się z siecią Tor (to, czym jest ta sieć, dokładnie wytłumaczone jest w drugim rozdziale).

Już w jednym z pierwszych wywiadów (w książce znajduje się około 30 wywiadów przeprowadzonych przez autorkę) czytamy „Wyśledzenie internauty w Torze rzeczywiście nie jest łatwe, ale możliwe. W internecie pokutuje przekonanie, że Tor jest w pełni bezpieczny, jeśli chodzi o ukrycie adresu IP. Tak jednak nie jest; ludzie popełniają błędy, które umożliwiają nam dotarcie do przestępców" (s. 41). W następnym rozdziale możemy przeczytać, że „Wrażenie anonimowości w internecie obecnie pozostaje tylko iluzją" (s. 51). Dowiadujemy się, jakie informacje są o nas zbierane przez różne firmy, w jaki sposób oraz ile informacji sami przez nieuwagę dobrowolnie przekazujemy. Rozdział ten napisany jest ku przestrodze, przez co w wielu momentach możemy mieć poczucie, że dane są analizowane jednostkowo, a nasze

wiadomości i maile czyta „jakiś pan w USA". Nie do końca jednak tak jest – Google Analytics faktycznie daje duże możliwości zbierania informacji na temat użytkowników danej strony; nasze maile są „czytane" przez boty (nie ludzi) w poszukiwaniu słów kluczowych, aby lepiej dopasować reklamy. Owszem, powstają potężne algorytmy, które biorą pod uwagę nasz wiek, płeć, znajomych czy nawet pogodę i dzień tygodnia. Jednak jest to wiedza analizowana na podstawie metodologii ilościowej – nie liczy się jednostka, a grupa, tworzenie modeli klienta sklepu. Autorka podkreśla, że w dzisiejszym świecie nie jesteśmy w stanie od tego uciec, ale ważna jest świadomość, jak te dane są wykorzystywane. Dla wzmocnienia przekazu zamieszczone są w książce trzy wywiady z programistami, którzy jednoznacznie mówią, że powinniśmy chronić naszą anonimowość, a myślenie – „nie mam co ukryć, więc nie mam nic przeciwko braku anonimowości" to „stanowisko o tyle głupie, co krótkowzroczne" (s. 60).

Kolejne rozdziały przedstawiają nam społeczności Anonymous, hakerów czy trolli. Dowiadujemy się, kim są, jak się kontaktują, poznajemy również ich historie, ponadto autorka dzieli ich na grupy ze względu na pewne typy osobowościowe. Wszystkie te społeczności są bardzo mocno ze sobą połączone. Zazwyczaj są to młodzi ludzie, którzy potrafią programować lub dopiero się tego uczą. Jak pisze Misha Glenn (dziennikarz i pisarz znający środowisko hakerskie), powinniśmy pamiętać, że „gdy rozwijali te zdolności hakerskie, ich moralność nie była jeszcze rozwinięta" (s. 209), co sugeruje, że powinniśmy pomóc takim ludziom, a nie wysyłać ich do więzienia za przestępstwa internetowe. W książce czytamy na temat wpływu tych grup na Arabską Wiosnę (2010 rok), ich możliwości technicznych czy politycznych. Temat demokracji w obliczu cyfryzacji jest kilkukrotnie poruszany. Przytaczana jest „doktryna" Googla: „Jeśli da się łączność i narzędzia do jej wykorzystania, demokracja wydarzy się sama" (s. 89), ale też fakt użycia trolli do celów politycznych przez rząd rosyjski. Cytowany w książce Napoleon Bonaparte mówi: "Wojna w 90% jest informacją" (s. 114). Dlatego też znajdziemy w książce wiele przykładów informacji, które wspomniane grupy uzyskały nielegalnie i udostępniły ogółowi społeczeństwa, aby pokazać przekręty i walczyć ze złem. Jak pisze jeden z respondentów: "Trolle nie wygrają wojny informacyjnej, ale ją wspomagają" (s. 122).

Oczywiście autorka pokazuje i tych „dobrych" i tych „złych". Tych, którzy włamują się do systemów informatycznych, wierząc, że zmieniają świat na lepsze, oraz tych, którzy zajmują się tym dla celów komercyjnych. Z raportu Cyber Security Breaches Survey z 2017 roku wynika, że prawie połowa przebadanych firm znajdujących się na terenie Wielkiej Brytanii w ciągu minionych 12 miesięcy została zaatakowana przez hakerów, z różnymi skutkami. Aż dla 35% firm niskim priorytetem jest bezpieczeństwo sieci wewnętrznej[1].

Z wywiadów możemy się dowiedzieć, jakimi pobudkami kierują się poszczególne grupy, oraz jak wygląda proces przygotowania się do ataku. Możemy uznać te grupy za ekskluzywne, ponieważ, jak odpowiadał jeden z respondentów: "Jedyna możliwość dołączenia do danej drużyny haktywistów, to polecenie przez ich członka". Co ciekawe, inny respondent pisze: „Tak, mamy więź (…), czuję ją nawet przez sieć" (s. 87). Mimo braku kontaktu ze światem realnym grupy potrafią rozpoznać swojego członka przez czas odpowiedzi, przerwy w wypowiedzi czy składnię. Według mnie ten wątek może zaciekawić nie tylko socjologów czy kulturoznawców, lecz także lingwistów. Dla językoznawców najciekawszy powinien być temat trolli, których poczucie humoru, liczba tworzonych przez nich neologizmów czy sposób prowadzenia konwersacji mocno odbiegają od codziennych rozmów.

Kiedy przyjrzymy się podrozdziałowi *Cenzopapy* – memów mówiących, że papież Polak był pedofilem – dowiadujemy się, że jest to nie tylko sposób na wywołanie burzy w internecie i naśmiewanie się z irytujących się ludzi w komentarzach pod postem. To również głębszy przekaz, mający mówić o problemie pedofilii w Kościele, choć bez oskarżania papieża o takie czyny.

1 https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2017 (dostęp 28.06.2018)

Najtrudniejszym rozdziałem do przeczytania jest *Cyberbullying*. Trudność ta nie wynika jednak z długości czy trudnego słownictwa, ale z powagi tematu. Autorka odwołuje się do badań prowadzonych przez NIK na ten temat cyberprzemocy w szkołach. Wyraźnie wskazują one, że „z cyberprzemocą zetknęło się prawie 40 proc. uczniów, blisko 30 proc. rodziców oraz 45 proc. ankietowanych nauczycieli (…). Blisko połowa ankietowanych uczniów stwierdziła, że w przypadku doświadczenia cyberprzemocy nie zwróciłaby się do nikogo o pomoc, nieco ponad 13 proc. uczniów zwróciłoby się o pomoc do nauczyciela, a 19 proc. do rodziców"[2].

Wyniki podkreślają wagę tematu i konieczność walki z tym przestępstwem. W książce czytamy autentyczne historie samobójstw spowodowanych cyberprzemocą. Z wywiadów możemy wyczytać, że na przemoc narażony jest każdy, kto nie wpasowuje się w standardy przyjęte przez dzieci w klasie (jest biedniejszy, mądrzejszy, grubszy etc.). Na koniec rozdziału znajdziemy listę linków do miejsc, które mówią o tym temacie, starają się edukować, pomagać ofiarom cyberbullyingu.

W kolejnym ciemnym zaułku internetu czekają na nas oszuści, którzy żerują na naiwności ludzi, tak samo jak w świecie realnym. Jak czytamy w książce *Sztuka podstępu; Łamałem ludzi nie hasła*, to socjotechnika często jest kluczem do bazy danych. Same umiejętności techniczne nie wystarczają.[3]

Spam 409 to z kolei metody „na wnuczka" w wersji mailingowej. Oszust musi nas przekonać, że jest naszą bliską rodziną oraz że potrzebuje pomocy. Wszelkiego rodzaju wirusy typu „malarl" szyfrują dane zamieszczone na dysku, a jedynym sposobem odblokowania jest zapłata okupu. Co ciekawe, autorka pisze, że tutaj oszuści są profesjonalni i często rzeczywiście odblokowują wtedy dane. Najciekawszym typem wirusa opisanym w książce jest „popcorn time", który „daje ofierze siedem dni na zapłacenie okupu, zanim zostaną skasowane jej pliki lub… roześle wirus dalej. Jeśli wirus pobierze i zainstaluje wirus – twoje pliki zostaną ci zwrócone" (s. 169). Jak postępują zaatakowani ludzie? Czemu tak, a nie inaczej? W jakim czasie podejmują decyzje? Jest to według mnie wątek do wielu rozważań.

Rozdział na temat hakerów pokazuje również inne zjawiska, które mogą wywołać naprawdę poważne konsekwencje dla danego kraju, od „Kali Linux", który został stworzony specjalnie dla grup radykalnych islamistów, aby mogli się wymieniać informacjami bezpiecznie i anonimowo, aż po takie akcje jak wirus „Stexnet", który zaatakował irańską elektrownię atomową.

Pod koniec książki możemy dowiedzieć się, jak powstał pierwszy największy narkotykowy rynek (*silk road*) znajdujący się po stronie darknetu. Historia jest długa i zawiła, ale najważniejsza jest końcówka rozdziału, która nie tylko ponownie mówi: programiści to też ludzie, więc popełniają błędy; i nawet jeśli korzystają z sieci Tor, to pewnego dnia odpowiedzą za swoje przestępstwa; znajdujemy tu również podrozdział mówiący o tym, jak wygląda analogiczna sytuacja po stronie clearnetu, jak proste jest kupienie narkotyków bez znajomości Tora. Ponownie widzimy, że internet złych rzeczy to nie tylko darknet.

Przedostatni rozdział poświęcony jest badaniom nad pedofilią w internecie. Autorka udawała 12-letnią dziewczynkę wchodzącą na forum i czekała na reakcje użytkowników. Mimo że dziennikarka wchodzi na zwykłe forum, a nie zamieszczone w darknecie, dostaje wiele ofert od starszych mężczyzn z propozycją seksu lub innych czynności seksualnych. W książce przytoczona została również afera, którą znajdziemy na Twitterze pod hasztagiem #twittergate, która nagłośniła problem zdjęć małych dzieci ubranych jedynie w bieliznę, często zamieszczanych przez nieświadomych rodziców, a później wykorzystywanych przez pedofili.

Książkę kończy seria wywiadów na temat przyszłości internetu. „Przyszłość internetu moim zdaniem jest jasna – coraz więcej osób będzie korzystać z zasobów sieci i będzie coraz szybszy dostęp do coraz większej ilości danych" (s. 301). Cała książka opisuje w wielu miejscach rzeczywistość, która dopiero buduje się w Polsce, jak choćby *internet of things*.

2 https://www.nik.gov.pl/aktualnosci/nik-o-cyberprzemocy-wsrod-dzieci-i-mlodziezy.html (dostęp: 28.06.2018)

3 Mitnick K, Simon W, (2003), *Sztuka podstępu; łamałem ludzi nie hasła, wydanie II*, Gliwice: Helion (s. 16–29, 201–223)

Na pytanie o anonimowości i internet złych rzeczy ciekawie odpowiada jeden z respondentów: „Celowo nie piszę o żadnych zagrożeniach związanych z anonimowością w sieci, bo to pozorny straszak, akurat najwięcej szkody wyrządzają ludzie (…) Najwięcej nienawiści leje się na Facebooku, a tam ludzie są pod nazwiskiem i jakoś ich to nie powstrzymuje" (s. 300). Autorka dodaje na koniec: „Ani Tor, ani VPN, ani anonimowość nie są potrzebne, aby robić złe rzeczy w internecie" (s. 307).

Należy podkreślić, że recenzowana książka nie należy do literatury naukowej. Brakuje w niej terminologii, oparcia o literaturę i teorię. Jednak jest to pozycja, która otwiera socjologowi wiele drzwi. Wskazuje punkty, które mogą zaciekawić grono naukowe, jak wcześniej już wspomniany wirus „popcorn", który stwarza nową płaszczyznę analizy relacji społecznych. Książka opisuje również społeczności internetowe, kategoryzuje je, tworzy typy, które według mnie mogą zostać rozwinięte i przeniesione na grunt naukowy. Troll klasyczny, hybrydowy, spiskowo-konspiracyjny, agresywny, encyklopedyczny – to nie jest podział, który znajdziemy w świecie nauki, ale wyniesiony z środowiska, przedstawia on, jak same grupy się określają i przypisują.

Wywiady i historie są świetnym materiałem, a zebrana literatura i raporty mogą się przydać w niejednej pracy akademickiej na temat cyberprzestrzeni. Książka ma również walory edukacyjnie. Nie tylko uświadamia czytelnika o zagrożeniach i o tym, jak wiele dzieje się w przestrzeni internetowej, lecz także podaje też wskazówki, jak można się chronić. To, do czego można mieć zastrzeżenia, to lekka hiperbolizacja problemu związaną z analizowaniem danych przez firmy. Ponadto również słownika, który znajduje się na początku książki, nie możemy traktować jako wartości samej w sobie. Wiele wytłumaczeń ma błąd logiczny (*idem per idem*), np. kuc (programista) – „kucem nazywa się osobę zajmującą się programowaniem. Ktoś może kucować, czyli programować" (s. 17), ale co ma kucanie do programowania? Opracowane hasła odnoszą się do wąskiego rozumienia danego słowa lub są błędnie interpretowane przez autorkę. Nie wiem, na jakiej podstawie zostały wyjaśnione, ale z własnego doświadczenia oraz z rozmów z kilkoma ludzi ze świata hakerów, wykopu itd. wiem, że inaczej rozumiemy połowę tych słów.

Odwołując się do cytatu, który otwierał tę recenzję, osobiście uważam, że jest on trafny, i pokazuje to ta książka. Ludzie nie myślą o konsekwencjach, udostępniają wiele zbędnych informacji, kreują swoją markę w internecie w rzeczywistości negatywnie, na przykład pokazując zdjęcia, na których są pijani, a na końcu dają się podejść i oszukać. Z badań NIK, które przytoczyłam, wynika, że tylko 19% dzieci w przypadku doświadczenia cyberprzemocy, zwróciłaby się do rodziców. Wiedza zawarta w książce *Internet złych rzeczy* jest potrzebna zwykłemu czytelnikowi, rodzicowi, aby widział, że dla nich to nie darknet, ale przede wszystkim clearnet może być zagrożeniem.

Mam nadzieję, że mimo braku włączenia książki *Internet złych rzeczy* w kategorie naukowe praca ta, również dzięki niniejszej recenzji, zostanie dostrzeżona jako pozycja, z której my, socjolodzy, kulturoznawcy czy lingwiści, możemy czerpać inspirację i wiedzę na temat świata, który jest tylko pozornie przez nas znany.

BIBLIOGRAFIA:

Cyber Security Breaches Survey 2017. *www.gov.uk/government/statistics/cyber-security--breaches-survey-2017.* (dostęp 28.06.2018)

Mitnick K., Simon W. (2003). *Sztuka podstępu łamałem ludzi nie hasła*, wydanie II. Gliwice: Helion.

Najwyższa Izba Kontroli. NIK o cyberprzemocy wśród dzieci i młodzieży. *http://www.nik.gov.pl/aktualnosci/nik-o--cyberprzemocy-wsrod-dzieci-i-mlodziezy.html* (dostęp: 28.06.2018)

Jagoda Czerwiec

Jagoda Czerwiec – socjolożka oraz UX designer, z internetem związana od zawsze. Pracuje obecnie w Fundacji Wielka Orkiestra Świątecznej Pomocy. Od kilku lat współpracuje z Katedrą Socjologii Ogólnej i Antropologii Społecznej AGH.