

Nemateria Konstitucio: La Post-Snowden Prizorgado de la Interreto

Harry Halpin

Abstraktaĵo: La demando ĉu rajtoj povas esti devigitaj per kodo subestas la bontenadon de Interretaj protokoloj fare de la IETF post la malkaŝoj de Snowden pri amasa gvatado de la NSA. Argumentoj pri la atendoj de uzantoj pri aliro kaj privateco inter la respektivaj inventintoj de la Reto kaj la Interreto metis la bazon por nova koncepto de retaj rajtoj bazita sur la tezo de plilongigita menso. Kelkaj leĝdonaj iniciatoj provis formi "Magna Cartan" por la Reto por devigi ĉi tiujn novnaskitajn retajn rajtojn, kiel ekzemple la rajton al privata komunikado, sed ĉi tiuj klopodoj unuforme malsukcesis. Tamen la riparo kaj bontenado de la teknikaj normoj de la Interreto mem fare de la IETF produktis novan specon de imanenta konstitucio por la Interreto bazita sur la uzo de kriptografio por defendi ĉi tiujn rajtojn.

Ŝlosilvortoj: Interreto, normoj, ĉifrado, bontenado, rajtoj

1. Enkonduko

La demando pri kiel la Interreto mem estas prizorgata, kaj kiu prizorgas ĝin, fariĝas plej grava dum la homaro fariĝas pli kaj pli dependa de cifereca infrastrukturo. La prizorgado de la Interreto povus esti konsiderata kiel sen pli vasta filozofia signifo, tamen la akceliĝanta ĉieesteco de la Interreto (ankaŭ simple nomata la "Reto") kaj pli vastaj ciferecaj teknologioj prezentas grandajn defiojn al filozofio, simile al kiel la invento de la Gutenberg-gazetaro kaj la sekva disvastiĝo de legopovo havis profundajn efikojn sur la filozofiajn demandojn, kiujn oni eĉ povis demandi tiutempe; finfine, "la mekanika spirito de moveblaj tipoj" havis sian "fidelan reflektan" en la filozofio de Descartes (McLuhan 2008, 244). En mondo profunde interplektita kun la Interreto, novaj filozofiaj demandoj estas prezentitaj, demandoj kun politikaj konsekvencoj: Ĉu teknikisto povas-

Harry Halpin, Nym Technologies kaj Vrije Universiteit Brussel, Place Numa-Droz 2, Pl. 2000
Neŭŝatelo, Svislando; hhalpin@ibiblio.org.



Techné: Esplorado en Filozofio kaj Teknologio

Ĉu socia sistemo malrespektas rajtojn, plifortigas ekzistantajn rajtojn, kaj eĉ kreas novajn konceptojn pri rajtoj? Se jes, kiu decidas pri kiaj precizaj rajtoj estas enkorpigataj de iu ajn teknologio: la projektistoj aŭ la finuzantoj? Aŭ ĉu ekzistas tria elekto: ĉu ĉi tiuj fortike politikaj decidoj povus esti faritaj de tiuj, kiuj prizorgas sistemon en sia ŝajne senpolitika laboro de bontenado kaj riparado? La detaloj de la respondo gravas, tiom kiom ili rivelas kiel uzantoj povas kaŭzi ŝanĝojn al teknikaj sistemoj laŭlonge de la tempo. En la kazo de la bontenado de la Interreto, la rolo de kodo en distribuado kaj ŝanĝado de sociaj rilatoj subtenas lastatempajn transformojn de suvereneco kaj rajtoj, kiuj historie estis konsiderataj ene de la sfero de politika filozofio.

Ĉi tiu jam menciita zorgo pri kiaj sociaj fortoj provokas ŝanĝon en artefakto aŭ sistemo post ĝia produktado estas la kerno de la filozofio de bontenado, kiu agnoskas la kreivan rolon, kiun bontenado kaj riparo ofte ludas en la subtenado de teknologioj laŭlonge de la tempo (Young 2020). Ĉi tio kontraŭdiras la enradikiĝintan ideon, ke la ĉefa tasko de bontenado estas malhelpi ŝanĝon aŭ restarigi la originalan telos de la inventinto fronte al paneo. Ĉi tiu akceptita vidpunkto pri teknologio baziĝas sur la klasika aristotela bildo de la inventinto-kiel-artisto, kie "arta produktado antaŭsupozas la ĉeeston de la formo de la produkto en la animo de la artisto" (Aristotelo 1924, 180). En la populara imago, la Interreto havas du inventintojn: Vint Cerf kaj Robert Kahn. Dum ĉi-lastata malaperis en la ombrojn de registara esplorado, Cerf nuntempe estas reprezentanto de Google. Kontraste, la TTT havas unuopan inventinton, Tim Berners-Lee, la fondinton de la normiga korpo kiu regas la normojn de la TTT, la Tutmonda TTT-Konsorcio (W3C).¹ Ĉu iliaj intencoj gravas fronte al la hodiaŭa komplekseco de la TTT? Transirante la aristotelan bildon de la inventinto, teknologio povas esti konsiderata kiel la konverĝo de socie elektitaj kriterioj — kriterioj de akceptebleco — kiuj kunigas ensemblon de teknikoj kaj artefaktoj en teknikan sistemon, igante la teknologion mem finfine ĉiam soci-teknika prefere ol pure teknika sistemo (Boris et al. 2018).

Post kiam teknologio estas establita, bontenado povas postuli konkretajn ŝanĝojn en teknika sistemo por konformigi ĝin al ŝanĝoj en la kriterioj de akceptebleco de uzantoj, aŭ simple al la kapablo de la teknika sistemo kontentigi ekzistantajn kriteriojn kiam ĝi estas alfrontita kun ŝanĝiĝanta mondo. Sen tia bontenado, la teknologio mem povas malsukcesi funkcii socie simple per malfunkciado. Tial, nia koncepto pri bontenado kaj riparado devas inkluzivi la agadon ŝanĝi, eble radikale, teknikan sistemon tra la tempo por ebligi al la sistemo resti uzata dum ŝanĝoj en la kriterioj de akceptebleco donitaj de ĝia...

Nemateria Konstitucio: La Post-Snowden-a Prizorgado de la Interreto

uzantoj, same kiel historiaj ŝanĝoj en materiaj kondiĉoj, kiuj ŝanĝas kiel tia sistemo estas uzata. Por konkretigi ĉi tiun punkton, ni prenas kiel nian paradigman kaz esploron la riparon de la Interreto post la malkaŝoj de Snowden pri amasa gvatado de la NSA, ĉar ĉi tiu krizo subfosis la atendon de uzantoj, ke la Interreto konservu ilian rajton al privateco.

Por situigi nian kaz esploron, ni skizas la rilaton inter teknologio kaj la teorio de la plilongigita menso, kiu provizas filozofian bazon pri kiel rajtoj kiel privateco povas esti enskribitaj en teknologion, kaj kiel tio kondukis al konflikto pri la nocio de "retaj rajtoj" inter Cerf kaj Berners-Lee, provokita de la interretaj ĉesigoj de la Araba Printempo. Poste ni skizos filozofian teorion pri normoj kaj protokoloj antaŭ ol detale priskribi la normigan procezon de la Interreta Inĝeniera Speciala Grupo (IETF). Kiel neformala internacia normiga instanco kun tia vasta atingo, la IETF estis nomita la "nemateria aristokrataro" de la Interreto (Halpin 2008). Post la revelacioj de Snowden pri amasa gvatado fare de la registaro de Usono, la agoj de la IETF montras kiel la filozofiaj debatoj pri retaj rajtoj kaj uzantaj atendoj estis solvitaj praktike per la deplojo de kriptografiaj protokoloj fare de la prizorgantoj de la Interreto, ne ĝiaj inventintoj. Efektive, ni trovas, ke grandparte estas la akcepteblaj kriterioj de uzantoj, kiuj pelas la prizorgadon de normoj, kiel mediaciite de inĝenieraj instancoj kiel la IETF. Fine, malgraŭ ke ĝia interna funkciado estas nekonata al la vasta plimulto de retuzantoj, ĉi tiu provo de IETF formi "nematerian konstitucion" per teknologio havas gravajn konsekvencojn por la nocio mem de rajtoj en tute cifereca epoko, same kiel por ajna teknologio, kies bontenado estas tereno de lukto, de publikaj transportsistemoj ĝis artefarita inteligenteco (AI).

2. De la Ret-Etendita Menso ĝis Retaj Rajtoj

La kreado kaj konservado de rajtoj per pure teknikaj rimedoj ŝajnas esti dubinda propono unuarigarde. En unu populare akceptita vidpunkto pri rajtoj, fundamentaj rajtoj estas konsiderataj transcendaĵoj al la homa kondiĉo, kiel en la kazo de la rajtoj donacitaj de Dio, naturo aŭ la ŝtato al individuo, kaj ilia deklaro kaj realigo lasitaj al eksplicite politikaj institucioj kiel la nacio-ŝtato kaj iliaj tribunaloj. Tamen, se teknologio povas efektive ŝanĝi la kognan konstitucion de la individuo, povus tre bone esti implicoj por nia nocio pri rajtoj. En konata filozofia argumento, Andy Clark kaj David Chalmers proponas en la tezo pri plilongigita menso, ke sub certaj kondiĉoj "la menso etendiĝas en la mondon" (1998, 12). Ilia klasika ekzemplo estas tiu de Otto, kiu suferas

Techné: Explorado en Filozofio kaj Teknologio

pro Alzheimer-malsano kaj tial povas navigi al lokoj kiel la Muzeo de Moderna Arto nur per notado de la instrukcioj en kajero, kiun li poste povas aliri laŭpete por plenumi la taskon. Clark kaj Chalmers deklaras, "La informoj en la kajero funkcias same kiel la informoj konsistigantaj ordinaran neokazantan kredon; simple okazas, ke ĉi tiuj informoj kuŝas preter la haŭto" kaj tial, iom da la kognativa merito apartenas al la artefakto, kondukante al la teoria demando: "Ĉu mia kognativa stato estas iel disvastigita tra la Interreto?" (Clark kaj Chalmers 1998, 17).

Malproksime de esti nur penseksperimento, ekzistas analoga realmonda kazo rilate al la Interreto: Diakono Patrick Jones perdis multon el la uzo de sia propra memoro "rezulte de traumata cerbolezo, tamen li vivas surprize normalan vivon kiel katolika diakono en Colorado Springs pro sia uzado de la reto kaj preta programaro, kiu permesas interligi, konservi, serĉi, preni kaj diagrami siajn proprajn pensojn, decidojn, kontaktojn kaj interagojn" (Berners-Lee kaj Halpin 2012, 4). Ĉar lia memoro mem estas etendita en la Interreton, ĉu havus sencin kalkuli ĉi tiujn etenditajn kapablojn donitajn de la Interreto kiel parton de liaj personaj kapabloj, metante tiujn el liaj memoroj konservitaj en la Interreto sur la saman nivelon kiel tiuj memoroj en lia kranio? Eble eĉ tiuj el ni sen memordamaĝo pli kaj pli similas al Deacon Jones, tiom kiom ni pli kaj pli serĉas aferojn en la Interreto anstataŭ memori ilin kaj uzas la Interreton por plenumi ĉiajn ĉiutagajn taskojn (Clowes 2013).

Tiaj ekzemploj signalas la eblecon de reto-etendita menso, kvankam la precizaj kondiĉoj sub kiuj kognativa etendo okazas estas ankoraŭ temo de intensa filozofia debato (Smart 2017). Se la Interreto estas kunkonstituanta de la menso, eĉ se nur en malforta senco kiel donite de distribuita pensado (Hutchins 1995), tiam la eĉ plia demando pri ĉu fundamentaj rajtoj devus esti etenditaj en la teknikan infrastrukturon mem estas sufiĉe nature provokita de ĉi tiu kognativa dependeco.

La demando pri la rilato inter teknika infrastrukturo kaj rajtoj estis puŝita sur la mondhistorian scenon per la ĉesigo de la Interreto dum la egipta revolucio de 2011. Unuiĝintaj Nacioj publikigis raporton alvokante, ke aliro al la Interreto estu konsiderata kiel netuŝebla homa rajto, kun Frank LaRue deklara: "Devus esti kiel eble plej malmulte da limigo al la fluo de informoj per la Interreto" (2011, 4). Tio kondukis al respondo de Cerf, provoke titolita "Aliro al la Interreto ne estas homa rajto", en kiu li argumentis, ke rajtoj kiel privateco kaj la rajto je aliro al la Interreto estas eblaj civitanrajtoj prefere ol necesaj fundamentaj homaj rajtoj, kiel homaj rajtoj estis deklaratitaj de Unuiĝintaj Nacioj.

Nemateria Konstitucio: La Post-Snowden-a Prizorgado de la Interreto

kaj tial devas esti efektiva de ĉiu ŝtato sendepende de iu ajn aparta teknologio (2012).

Tamen, la mallarĝa kompreno de Cerf pri fundamentaj rajtoj kiel senŝanĝa aro da rajtoj, kiuj, malgraŭ sia ŝajne senhistoria transcendo, estis deklaritaj unufoje kaj nur unufoje de UN, provokis refuton de Berners-Lee kaj Halpin titolitan "Defendu la Reton", kie oni argumentas, ke nur se "ni komencos paroli pri aliro al la kapabloj de la Interreto rilate al homaj rajtoj", tiam "ni povas imagi, ke diversaj registaroj povus subteni ilin kiel rajtojn" (2012, 6). Bazante sian argumenton sur la tezo de plilongigita menso (Clark kaj Chalmers 1998), Berners-Lee kaj Halpin asertas, ke se la Reto estas etendaĵo de la menso de persono, tiam la rajtoj de persono pri siaj datumoj en la Reto devus esti ekvivalentaj al la rajtoj donitaj al la korpo kaj menso de la persono ekster la Reto, tiel ke fortranĉi la aliron al la Reto malobservas la integrecon de la menso de individuo. Ĉi tiu argumentaro kondukas al la konkludo, ke la rajto aliri la Reton povus esti konsiderata nova speco de rajto, ĉar ĝi koheras kun la atendoj de kreskanta parto de la homaro (Berners-Lee kaj Halpin 2012). Ĉi tiu pleda linio de Berners-Lee kondukis al la amorfa ideo de retaj rajtoj, nova klaso de rajtoj - intervalantaj de la rajto al interreta aliro ĝis la rajto al privata komunikado - validantaj por homoj pro la etendo de la kognaj kapabloj super la Interreto. Vere, Cerf ankaŭ argumentis, ke estas "la respondeco de la kreintoj de teknologio mem subteni homajn kaj civitanajn rajtojn", ĉar "estas inĝenieroj - kaj niaj profesiaj asocioj kaj normigaj instancoj [...] - kiuj kreas kaj konservas ĉi tiujn novajn kapablojn" (2012, 26). Sendepende de ĉu rajtoj estas konsiderataj historiigitaj aŭ sentempaj el la vidpunkto de filozofio, ĉi tiu debato elstarigas la demandon, ĉu rajtoj povas esti enkorpiĝitaj en teknologio, eĉ en la ŝajne rutina bontenado de teknika normigado.

3. Protokoloj, Lingvaj Ludoj, kaj la Interreto

Teknikaj normoj estas substudataj en la filozofio de bontenado, malgraŭ kreskanta intereso en sociologio kaj antropologio (Yates kaj Murphy 2019; Ten Over 2021). Teknikaj normoj ne estas filozofie senkulpaj, ĉar ili povas enkorpiĝi apartajn kaj eĉ strangajn filozofiajn poziciojn. Ekzemple, en la kampo de Interretaj normoj, Berners-Lee asertas, ke la signifo kaj referenco povas esti rigide indikitaj per identigiloj en la Reto, polemika pozicio antaŭe esplorita teorie de la filozofio de lingvo en la debatoj pri propraj nomoj (Monnin kaj Halpin 2012). Ĉar la funkciado de la Interreto estas tipe difinita per komputilaj programoj, kiuj konkretigas abstraktajn interretojn...

Techné: Explorado en Filozofio kaj Teknologio

retnormoj, kompreni la filozofian signifon de la Interreto postulas pli profundan ekzamenon de la rolo de normoj (Halpin 2008).

En tiu ĉi senco, ni supozas, ke teknikaj normoj estas konvencioj, kiuj esprimas regulecojn en la gamo de eblaj agoj, nomataj la protokolo, de klaso de teknikaj artefaktoj, kiuj en la kazo de la Interreto estas komputilaj programoj. Oni povas konsideri protokolojn por specifi movojn en lingva ludo por komputile mediaciita komunikado per programoj, rememorigaj pri la lingvaj ludoj de la malfrua Wittgenstein, inkluzive de ilia neredukteble socia naturo, tiom kiom la lingva ludo mem aktive ŝanĝiĝas laŭlonge de la tempo pro la agoj - tio estas, la vivoformoj - de la partoprenantoj (Wittgenstein 1953). Oni povus argumenti, ke komputiloj ne povas partopreni en lingvaj ludoj, ĉar al ili mankas vivata socia mondo, kaj protokoloj estas nur senŝanĝaj instrukcioj por maŝinoj sen ia ajn fenomenologia ekzisto. Tamen, ĉi tiu simplisma analizo de protokoloj ignoras la socian enradikiĝon de komputado, inkluzive de iliaj efikoj sur homan fenomenologion. Kiel Langdon Winner diris, teknologioj kiel komputiloj "interplektiĝas en la teksturon de ĉiutaga ekzisto" kaj "la aparatoj, teknikoj kaj sistemoj, kiujn ni adoptas, perdas siajn il-similajn kvalitojn por fariĝi parto de nia mem homeco", tiel strukturante nian vivformon (2014, 55). Eĉ pli foren, komputilaj protokoloj estas neredukteble sociaj, ĉar ili estas kreitaj, konservitaj, riparitaj kaj celoj.

Ĉi-punkte estus utile memori la diferencon inter formalaj lingvoj kaj naturaj lingvoj. Formalaj lingvoj, kiel matematikaj esprimoj kaj programlingvoj, havas kondutojn, kiujn oni povas precize difini kaj tiel efektiviĝi mekanisme. Homaj lingvoj estas nomataj naturaj lingvoj por distingi ilin de formalaj lingvoj. Dum lingvaj ludoj donitaj per la uzo de natura lingvo estas implicate dependaj de la konkreta situacio, komputilaj protokoloj povas esti mekanisme efektivitaj sendepende de la specifa enigita kaj enkorpigita situacio de la komputilo. Tamen, ĉi tiu supozebla opozicio inter formalaj lingvoj kaj naturaj lingvoj ne validas je la nivelo de kreado kaj uzo de protokoloj fare de homoj, kiel ekzempligite per teknikaj normoj. Teknikaj normoj estas priskriboj de formalaj protokoloj en la natura lingvo de teknika prozo (tro ofte en la angla) kun tiom da aŭ tiom malmulte da formala notacio kiom necesas por ke programistoj ĝuste efektivigu la protokolon. Teknika normo estas ia receptolibro por efektiviĝi protokolon, do ekzistas varia grado da formaleco kaj abstraktado trans malsamaj normoj. Por preni ekzemplon de ĉi tiu varianco en abstraktado, la tavoloj de la Interreto — de la "Fizika" ĝis la "Reta" ĝis la "Aplika" nivelo — estas

Nemateria Konstitucio: La Post-Snowden-a Prizorgado de la Interreto

donitaj kiel sep tavoloj de la normo Open Systems Interconnection (OSI) specifita de la serio de teknikaj normoj X2.00 de ITU (Internacia Telekomunika Unio).² Kontraste, la IETF difinas nur kvar tavolojn en sia RFC 11223 kaj la normoj RFC 11234.

Ĉu normo sukcesas aŭ ne dependas de ĉu ordinaraj homaj programistoj povas, per legado de la normo, krei programon kies konduto konformas al ĝi. La celo de normo estas certigi, ke aparte efektivigitaj komputilaj programoj povas komuniki per la protokolo, tiel ke ilia konduto povas esti antaŭdirita el la reguloj donitaj de la normo (Clark 2018). Por plu alvoki Wittgenstein, ĉi tiu konduto ne povas esti antaŭdirita kun absoluta certeco, ĉar la reguloj ne estas plene formaligitaj kun ĉiu ebla situacio konsiderata anticipe (1969). Anstataŭe, la reguloj estas gvidlinioj, kiuj reflektas socian interkonsenton pri kiel protokolo devus konduki: "La vorto 'interkonsento' kaj la vorto 'regulo' estas rilataj unu al la alia, ili estas kuzoj. Se mi instruas al iu la uzon de unu vorto, li lernas la uzon de la alia per ĝi" (1969, 73). Teknikaj normoj estas sociaj interkonsentoj inter efektivigantoj, kie la socia interkonsento estas farita per diversaj normigaj instancoj, kiuj poste provizas gvidliniojn por estontaj efektivigantoj.

Ankaŭ ekzistas konkurenco inter diversaj normigaj instancoj, kiuj produktas similajn normojn por la sama celo; por reveni al nia gvida ekzemplo, dum la OSI-referenca modelo estas difinita per la tre strukturitaj internaciaj ITU-procezoj, multaj el la protokoloj, kiujn ITU difinis por komputila retigado, ne estis vaste efektivigitaj, kaj la pli simplaj protokoloj proponitaj de la pli Uson-dominata IETF fariĝis pli vaste efektivigitaj.

Teknika normo ne estas nur socia interkonsento, sed interkonsento kiu ekvalidas per la deplojo de teknika sistemo kaj povas ŝanĝiĝi laŭ ĝia uzado. Por ke normo estu sukcesa, devus esti sufiĉe da antaŭvidebleco en konduto, ke normo-konformaj efektivigoj povu interagi per protokoloj por plenumi taskojn. La Reto konsistas el vasta gamo da normoj, kiel Dosiertransiga Protokolo (FTP) por elŭti dosierojn, Simpla Poŝttransiga Protokolo (SMTP) por retpoŝto, kaj Hiperteksta Transiga Protokolo (HTTP) por interagi kun retejoj. Teknikaj normoj ofte konstruiĝas unu sur la alia en ĉiam pli kompleksaj kombinaĵoj, kiel montras la fakto, ke multaj el la supre menciitaj funkcioj de la Reto estas nuntempe inkluditaj en la Reto per la senhalta vastiĝo de la funkcio de HTTP. Teknika normo povas lasi certajn aspektojn nedeterminitaj pro esti skribita en natura lingvo kaj esti specifita je certa nivelo de abstraktado, donante liberecon al efektivigantoj: Ekzemple, la HTML-normo, kune kun normoj kiel CSS (Kaskada Stilo)

Techné: Explorado en Filozofio kaj Teknologio

Folioj) kaj programlingvoj kiel Javascript difinas kiel retpaĝo estas bildigita per sendepende efektivigitaj retumiloj, de Safari de Apple ĝis Chrome de Google. Kvankam la retpaĝo devus esti bildigita laŭ la normo sendepende de la retumilo, la specifaj detaloj de la bildigo povas diferenci, baziĝante sur tio, kio estas havebla al la operaciumo, aparataro, ktp. Malsamaj programoj povas funkcii sur malsamaj operaciumoj donitaj en vasta aro da programlingvoj, sed kondiĉe ke normo estas sekvata, normkonforma programo povas komuniki kun aliaj normbazitaj programoj por plenumi pli vastajn taskojn. La programoj, kiuj konformas al normo, povas esti proprietaj aŭ malfermfontaj; kondiĉe ke ilia konduto estas antaŭvidebla ene de la intervalo postulata de la koncerna tasko, ne plu necesas "vidi interne" de la programo ol necesas "vidi interne" de la cerbo de alia homo por komuniki per natura lingvo.

Kun ĉiuj siaj diversaj ecoj kaj kapabloj, la Interreto povas esti difinita kiel universala reto, kie interoperaciebleco inter apartaj retoj eblas per aro da teknikaj normoj. Dum la originala normo de la Interreto, ne surprize nomita RFC 15 de la IETF, skizis kiel sendi informojn inter du komputiloj en la reto ARPA (Advanced Research Projects Agency) (ARPAnet), kiu estis la antaŭulo de la Interreto, estis RFC 6756 de Cerf kaj samlandanoj, kiu difinis la Interreton. RFC 675 establis TCP kiel universalan protokolon, kiu kapablas porti ajnan specon de datumoj inter komputiloj identigitaj per IP-adresoj, senlime de ĝia uzado fare de aplikaĵo, en klara kontrasto al pli fruaj normoj por komunikado per radioj kaj telefonoj (Lessig 1999). Tiel, komputiloj komunikantaj per la normo TCP/IP (Transmission Control Protocol/Internet Protocol) estas konsiderataj parto de la Interreto, sed komputiloj komunikantaj uzante nur proprietan protokolon kiel AppleTalk ne estus konsiderataj parto de la Interreto. Universaleco per normigita interoperaciebleco estas kerna al la Interreto, tiel ke ĉiu homo uzanta komputilon konektitan al la Interreto devus havi la saman aliron al diversaj kapabloj kaj rimedoj. Dum la Interreto penetras ĉiam pli en la mondon, ĉi tiu universaligo de kapabloj fariĝas pli kaj pli disvastigita kaj atendata de uzantoj, sendepende de ĉu la inventintoj de la teknologio konceptis ĉi tiujn kapablojn kiel enkorpiĝon de universalaj rajtoj aŭ ne.

4. La Interreta Inĝenieristika Speciala Grupo: La Prizorgantoj de la Interreto

Vizio de universaleco estas eneca en la Interreto, kaj la konkreta enkorpiĝo de ĉi tiu universaleco, kies specifeco estas senfina, estas donita de Interretaj normoj.

Nemateria Konstitucio: La Post-Snowden-a Prizorgado de la Interreto

kiuj simile ŝanĝiĝas laŭlonge de la tempo per la socia bontenado de protokoloj. Kontraŭe al la klasika dikotomio inter la kreiva kreado de teknika artefakto fare de inventinto kaj ĝia uzado fare de tiuj, kiuj nur utiligas ĝian funkciadon, ekzistas kreiva laboro, kiu okazas post kiam artefaktoj estas kreitaj, kaj ĉi tiu laboro povas esti influita - aŭ eĉ determinita - per uzado (Young 2020). Teknika normigo montras abunde, ke la laboro de bontenado iras "preter la formo origine antaŭvidita de la dizajnisto", ĉar la Interreto estas kontinue konsistigita de "procezoj, kiuj estas etenditaj kaj gvidataj tra la tempo per la agado de homaj agantoj" (Young 2020, 363–64). Ekzemple, la ĉefa normiga instanco de la Interreto estas la Interreta Inĝeniera Speciala Grupo (IETF), kiu fakte respondecas pri la kreado, bontenado kaj riparado de Interretaj protokoloj.⁷ Ekde la komenco de la Interreto, la celo de ĉi tiu malstrikta socia grupo estis produkti kaj konservi ĉi tiujn normojn per vage rekta demokratia kaj multkoncernata modelo de regado, kontraste al pli tradiciaj normigaj instancoj kiel ISO (Internacia Normorganizo), kiuj limigas sin al oficialaj koncernatoj de registaroj. Kontraste al la Interreto, la Tutmonda Reto (la "Reto") estas difinita de sia inventinto, Berners-Lee, kiel universala nomskemo nomata URL-oj, kio signifas "Universalaj Rimedo-Lokigiloj" por rimedoj (kiel hipertekstaj retpaĝoj) kiel difinite de IETF RFC 3986 (Monnin kaj Halpin 2012).⁸

Tamen, la TTT disbranĉiĝis de sia propra normiga instanco de la IETF: La W3C, kiu alprenis la formon de reprezenta demokratio de kompanioj sub la gvido de Berners-Lee kiel la IETF, ĉar la rekte demokratia decidiĝo de la IETF estis konsiderata tro malrapida kaj kaosa por la rapide evoluanta entreprena TTT.⁹ En realeco, la W3C fine traktis retumilajn normojn kiel HTML, dum retprotokoloj kaj la vasta plimulto de interretaj normoj restis ĉe la IETF, do praktike la TTT estas konsiderata subaro de la Interreto.

Mallonge resumante, la IETF ekestis baldaŭ post la kreado de la Interreto, kiu estis la produkto de grandskalaj akademias kaj militaj esplorstipendioj de la usona registaro por produkti distribuitan "intergalaksan" reton por dividi rimedojn inter komputiloj kun malsamaj proprietaj operaciumoj kaj retoj (Licklider 1963; Baran 1964). Esplorstipendioj de DARPA (Defenda Altnivela Esplorprojekto-Agentejo) produktis la necesajn komencajn dezajnoj de la ŝlosilaj protokoloj kiel TCP/IP, ankaŭ nomata la modelo de la "Departemento de Defendo", kiu poste elfazigis la plej fruan neformalan NCP (Reta Kontrola Programo) de ARPANet (Cerf kaj Kahn 1974). Nomante sin la Reta Laborgrupo, la efektivigantoj de ĉi tiuj protokoloj (plejparte diplomigintoj, inkluzive de Vint Cerf tiutempe) trovis, ke akademias artikoloj ne provizis la necesajn...

Techné: Explorado en Filozofio kaj Teknologio

nivelo de detalo por efektiviigi protokolon laŭ interoperaciebla maniero. Ili fine komencis afiŝi notojn pri kiel efektiviigi certajn protokolojn en la unua komunikada forumo de la Interreto, la oNLine Sistemo (NLS) de Douglas Engelbart.

Ĉar tiuj estis konsiderataj neformalaj notoj prefere ol oficialaj normoj ĉe

tiutempe, ili nomiĝis "Petoj por Komentoj" (RFC), termino kiu ankoraŭ estas uzata hodiaŭ de la IETF (Abbate 1999). La implikiĝo de kreskanta nombro da programistoj laborantaj por privataj kompanioj kondukis al la organizado de fizikaj kunvenoj ekde 1986. Ĉi tiuj kunvenoj estis esence malfermaj al ĉiu, male al la rigida normiga procezo de ISO kaj ITU, kie ĉiu nacio-ŝtato havis bone difinitajn reprezentantojn. Estas el ĉi tiu matrico, ke la IETF evoluigis sian rimarkinde malferman estraran strukturon, kiu permesis al ĉiu ajn ĉeesti kunvenon, afiŝi ideon por protokolo en dissendolisto kaj publikigi skizon de RFC.

La malferma naturo de la IETF estas esenca por kompreni kaj la kreadon kaj la bontenadon de Interretaj normoj. Post aprobo fare de la Interreta Inĝenieristika Steering Group (IESG), malsamaj temoj estas donitaj al la "Laborgrupoj" de IETF kun apartaj dissendolistoj. La IESG mem estas elektita de Nomuma Komitato elektita per lotumo el oftaj ĉeestantoj de la IETF-kunvenoj.¹⁰

Ĉiu ajn povas verki dokumenton en la IETF nomatan "Interreta Skizo". Se Laborgrupo adoptas Interretan Skizon, ĝi ricevas RFC-numeron kaj fariĝas "Laborskizo". Malklarigante la limon inter la kreado de normo kaj ĝia efektiviigo, ekzistas kontinua retrokupa buklo inter la fakta uzado de la programoj, kiuj pretendas efektiviigi la protokolon, kaj la teksto de la RFC mem, kiu difinas la protokolon. Ĉi tio kondukas al procezo de kontinua riparado de la ekzistanta natura lingvoteksto, tiel ke la teksto de la RFC atingas la ĝustan nivelon de abstraktado kaj detalo por priskribi la ekzistantajn efektiviigojn de la proponita normo. En la IETF, ĉiam ekzistas iu malkonsento pri la detaloj, sed konsento en la IETF estas prenita per argumentado en la dissendolisto aŭ per "zumado" ĉe persona IETF-kunveno. Ĉi tiu plejparte neformala procezo kutime daŭras ĉirkaŭ kvin jarojn por atingi ekvilibron pro la kontinua tien kaj reen inter la normoj kaj efektiviigantoj, kiuj raportas pri la uzado de la protokolo en la naturo fare de uzantoj. RFC estas tiam konsiderata "Proponita Normo" post kiam oni atingas konsenton ene de la Laborgrupo. Poste ĝi fariĝas "Interreta Normo" post kiam ĝi pasas revizion fare de altrangaj membroj de la IETF (Areaj Direktoroj), nomataj IESG, kiuj determinas ĉu la RFC devus esti vaste efektivigita kaj inda je esti normo. Tiel, la vasta plimulto de RFC-oj restas kiel Laborskizoj porĉiame, kaj Laborgrupoj fariĝas konstantaj instancoj.

Nemateria Konstitucio: La Post-Snowden-a Prizorgado de la Interreto

La kialoj de la sukceso de la IETF estas pli vastaj por la filozofio de bontenado. Responde al novaj kaj neantaŭvideblaj homaj sociaj bezonoj, novaj interretaj protokoloj estas bezonataj kaj pli malnovaj protokoloj povas rompiĝi aŭ elfali el uzo. La protokolo povas aperi unue, kaj poste esti normigita per RFC, aŭ la normo povas difini protokolon, kiu poste estas efektivigita en la naturo per multaj malsamaj programoj; dum ili estas prizorgataj kaj riparitaj laŭlonge de la tempo, la protokoloj kaj normoj fariĝas kunkonstituaj. Ĉar ilia adopto servas specon de objektiva taŭgeca funkcio, protokoloj evoluas en procezo pli simila al natura evoluo pelita de uzado ol al la aristotela nocio de inventinto kun tute intenca dezajno por protokolo "en sia kapo". Cetere, la sukceso, kaj do reproduktado, de protokolo estas difinita unue per ĝia adopto fare de efektivigantoj, kaj finfine la uzado de la protokolo fare de finuzantoj, prefere ol ĉu ĝi kontentigas la intencon de sia inventinto aŭ ne. La Interreto ne estas fermita teknika sistemo, sed malferma sistemo, kiu povas disetendiĝi kaj ĝisdatigi per novaj normoj. Tio igas la Interreton karakterizi per sia eneca generativeco, en kiu la generado de novaj kapabloj, de retumado ĝis fluado de video, ĉiuj neantaŭviditaj de ĝiaj originaj inventintoj, daŭras senĉese (Zittrain 2008). La malstrikta estrara strukturo de la IETF estas unike taŭga por ĉi tiu stilo de uzo-movita normigado, ĉar la IETF difinas procezon, kiu permesas al protokoloj ŝanĝiĝi kaj evolui laŭ maniero pli simila al homaj lingvoj ol al formalaj lingvoj, tamen sen rezigni pri la nocio de interoperaciebla normigado.

La IETF ne nur prizorgas la Interreton per la bontenado de ekzistantaj normoj kaj la kreado de novaj normoj, sed ankaŭ funkcias por ripari la erarojn de la komenca dezajno de la Interreto. La prapeko de la Interreto estis ĝia manko de sekureco. Ĉar la Interreto estis desegnita ĉe sia genezo en fidinda akademia medio, estis malmulte da bezono pri sekureco. Decide, kriptografio estis konsiderata ŝtata sekreto uzebla ĉefe de registaraj instancoj kiel la Nacia Sekureca Agentejo (NSA) de Usono, prefere ol de individuoj.

Fakte, kriptografio estis aktive kaŝita de tiuj ekster la registaraj koridoroj. Kiel raportite en la populara gazetaro (Leyden 2014), Cerf priskribis la situacion jene: "Mi laboris kun la Nacia Sekureca Agentejo pri la dezajno de sekurigita versio de la Interreto, sed ni uzis konfidencan sekurecan teknologion tiutempe kaj mi ne povis dividi tion kun miaj kolegoj. Se mi povus rekomenci, mi enkondukus multe pli fortan aŭtentigon kaj kriptografion en la sistemon." Berners-Lee ankaŭ ne sukcesis aldoni ĉifradon al la frua versio de la Reto, kiun li konstruis en la 1990-aj jaroj, malgraŭ ke publika ŝlosila kriptografio estis publike rivelita jardekojn antaŭe fare de Whitfield Diffie kaj Martin Hellman (1976).

Techné: Explorado en Filozofio kaj Teknologio

La celo de moderna kriptografio estas malhelpi neaŭtorizitan personon malĉifri ĉifritan mesaĝon kaj legi ĝian enhavon. Alivorte, persono povus sendi al specifa ricevanto mesaĝon, kiun nur la celita ricevanto povus legi per uzado de sia publika ŝlosilo por ĉifri la mesaĝon, ĉar nur la privata ŝlosilo de la ricevanto permesus la malĉifradon de la mesaĝo (Diffie kaj Hell-man 1976). La privata ŝlosilo estas tipe granda hazarda nombro, kun publika ŝlosilo derivita de la privata ŝlosilo per matematika operacio kiel ekzemple eksponenciado en finhavaj kampoj aŭ, pli lastatempe, operacioj en elipsa kurbo. Ekzemploj de kriptografiaj primitivoj inkluzivas haŝfunkciojn uzatajn por krei kriptografiajn unudirektajn "kompendiojn" (similajn al unika fingrospuro por datumoj) kiel la SHA (Sekura Haŝa Algoritmo) por ĉifraj algoritmoj kiel AES (Altnivela Ĉifrada Normo) (Smart 2016). Ĉi tiuj kriptografiaj primitivoj estis tipe deciditaj per malfermaj konkursoj ĉe naciaj instancoj kiel NIST (Nacia Instituto de Normoj kaj Teknologio) de Usono.

Ĉi tiu aldono de ĉifrado al kernaj interretaj protokoloj devis esti farita post-hoc fare de la IETF dum jardeko. Ĉiu protokolo devis havi sian originan laborgrupon reaktivigitan aŭ novan kreitan por fari sekuran version de ekzistanta, vaste deplojita protokolo. Mallonga superrigardo pri la tempo bezonata de la IETF por aldoni ĉifradon al la kernaj protokoloj de la Reto estas jena: TCP/IP (1981) al IPsec (1995), Telnet (1983) al SSH (1995), FTP (1985) al SFTP (1997), SMTP (1982) al OpenPGP (1991), kaj HTTP (1997) al TLS (1999). La aldono de kriptografio por devigi sekurecon en la Interreto, kiel postulite de uzado ekster la akademia mondo, estis ago de bontenado, tiom kiom ĝi estis necesa por ke la Interreto plenumu sian originalan dezajnon por interoperaciebleco, sed la uzado de la kriptografiaj normoj de IETF fare de la ĝenerala publiko restis malalta, escepte de TLS por retkomercaj retejoj. Ĉi tiu manko de sekureco en la Interreto kondukis al timo, ke okazos "9/11-okazaĵo" por la Interreto, kiu detruus la implican fidon, kiun multaj metis en la infrastrukturon de la Interreto (Zittrain 2008).

5. La Revelacioj de Snowden kaj la Demando pri Retaj Rajtoj

Kio okazas kiam la atendoj de la uzantoj de teknologio estas malobservitaj, kaj ĝis kia grado la inventintoj de teknologio povas reveni por gvidi sian originalan dezajnon tra la posta krizo? En 2013, Edward Snowden, iama NSA-dungito, pruvis - per likado de konfidencaj dokumentoj al la gazetaro - ke la tuta Interreto estis sub gvatado fare de sia iama dunganto (Snowden 2019).

La gvatado okazis en "escepta stato" bazita sur postulo post la 9/11 de la usona sekureca aparato por tuteca informa konscio sendepende de

Nemateria Konstitucio: La Post-Snowden-a Prizorgado de la Interreto

ekzistantajn leĝojn kaj normojn (Agamben 2005). Ĉi tio malobservis per pura teknika dekreto la formalan konstitucion de Usono, precipe la kvaran amendon (Mornin 2014). Dum gvatado de ĉi tiu skalo estis teoriadita de kriptografoj kaj privatec-aktivuloj dum jaroj (Diffie kaj Landau 2007), la realo de amasa gvatado estis pli granda ol la inĝenieroj de la IETF, same kiel entreprenoj kaj eksterlandaj registaroj, pensis ebla. Por la unua fojo, la ĝenerala publiko amase maltrankviliĝis pri la privateco kaj sekureco de la Interreto mem, ĉar la antaŭe nevideblaj normoj de la Interreto montriĝis ne certigi la privatecon atendatan de multaj el ĝiaj uzantoj (Snowden 2019). Ĉi tiu revelacio skuis la IETF ĝis ĝia kerno, ĉar multaj el ĝiaj membroj forte kredis je rajto al privateco (Ten Oever 2021). Pli malbone, Snowden ankaŭ malkaŝis la subfosadon de usona-registar-aprobitaj kriptografiaj normoj fare de la NSA, inkluzive de tiuj uzataj de la IETF, rektan ofendon al sekureca normigo (Snowden 2019).

Kiel esplorite de la filozofio de teknologio en kazoj kiel la sekureco de medicino (Feenberg 2017), sociaj supozoj estas enecaj en la kriterioj de akceptebleco, kiujn homoj alportas al sia ĉiutaga uzado de teknologio, eĉ se tiuj supozoj estas nuntempe malobservitaj en praktiko. Tiel, la kriterioj de privateco, kiujn uzantoj pensis esti garantiitaj por ilia komunikado tra la Interreto, fine estis malobservitaj de la NSA, kaj tio signifas, ke uzantoj jam ne fidis la teknikan infrastrukturon mem. Amasa gvatado signifas, ke preskaŭ ĉiu mesaĝo sendita tra la Interreto estis kaptita por fina prilaborado, unue per stokado de la enhavo de la mesaĝo kaj poste determinado de "kiu" komunikis kun "kiu" per retanalizo kaj maŝinlernado, eĉ se la enhavo de la mesaĝo estis ĉifrita (Appelbaum 2022). Multaj homoj racie atendas, ke ilia uzado de la Interreto estas privata; ekzemple, ke la interkapto de ilia retpoŝto fare de nekonataj triaj partioj estas protektita de la samaj rajtoj kiel ilia poŝto.

Tamen, en la plej multaj landoj ne ekzistas leĝoj kontraŭ la amasa gvatado de retpoŝto. Krome, la datencentroj konstruataj de la NSA — same kiel tiuj de privataj kompanioj — havas la potencialon stoki la enhavon de komunikadoj dum longaj, se ne senfinaj, tempodaŭroj.

Kvankam privateco ankoraŭ estas disputiga temo en debatoj pri homaj rajtoj kaj plena kalkulado estas ekster nia amplekso ĉi tie, tamen oni notu, ke privateco estis konsiderata de iuj kiel konstitua de esti homo kaj antaŭkondiĉo por la uzo de racio (Solove 2008). Uzante la saman argumenton per funkcia ekvivalenteco ekzempligita per la tezo pri etendita menso (Clark kaj Chalmers 1998), la rajto al privateco povus esti etendita al la Interreto por konservi homan aŭtonomecon en la Reto. Se ekzistas unu kazo, kie persono eble sentas, ke

Techné: Esplorado en Filozofio kaj Teknologio

iliaj pensoj mem turniĝas kontraŭ ili, temas pri misuzo de persono ebligita per gvatado de privataj kaj personaj datumoj. Antaŭaj filozofiaj laboroj sugestas, ke aliro - des malpli forigo - de eksteraj rimedoj necesaj por kognaj funkciado estas fundamenta malobservo de la mensa integreco de la persono (Palermos 2023). Por restarigi la fidon de uzantoj en la Interreto, io devis esti farita. La inventintoj de la Interreto kaj la TTT respondis ĉiu laŭ sia propra maniero al la krizo.

Ĉu la mondhistoria aŭro de la inventinto de teknologio povus konduki al la devigo de nova reta rajto je privateco, kiu povus fini tian misuzon? En marto de 2014, Snowden aperis "rekte" sur scenejo per teleĉeesta roboto kun Berners-Lee, kiu ĵus anoncis sian intencon lanĉi sian "Magna Carta por la Reto" por defendi la rajtojn de la ordinaraj uzantoj kontraŭ misuzoj fare de registaroj kaj teknologiaj kompanioj (Pitt-Brooke 2014). Konforme al la malpli konata frato de la Magna Carta, la Ĉarto de la Arbaro, ĉi tiu lukto pri retaj rajtoj povus esti konceptita kiel la lukto por la komunaj kaj bazaj rajtoj kontraŭ feŭdaj regantoj renaskitaj por la cifereca epoko (Linebaugh 2009). En praktiko, ĉi tiu alvoko de Berners-Lee por krei novan specon de konstitucio de la Interreto estis simple krei politikan traktaton inter la tekno-feŭdistoj de Silicon Valley kaj la pli grandaj nacio-ŝtatoj (kun amasgvataj kapabloj), kiu sanktigis retajn rajtojn en nacian kaj internacian juron, laŭ la spirito de la Magna Carta inter la feŭdaj regantoj kaj la angla monarkio.

Post Snowden, pluraj provoj kolektive akiri retajn rajtojn okazis je nacia nivelo, sekvante la sukcese kolektive efektivigitan Marco-Civilan Leĝon pri la Interreto en Brazilo¹¹ kaj la pli "desupre" Ĝeneralan Regularon pri Datumata Protekto (GDPR) kreitan en Eŭropo. Tamen, tio ne signifas, ke eksperimentoj pri kolektive akiri retajn rajtojn ne okazis en Eŭropo; Italio produktis Deklaracion pri Interretaj Rajtoj, publikigitan interrete de la Itala Deputita Ĉambro en 2014.¹² En 2015, la Cifereca Komitato de la Franca Nacia Asembleo komencis siajn proprajn proponojn por retaj rajtoj, prezentante cent rekomendojn kun pli ol 4 000 komentoj, inkluzive de la rajto al interreta aliro, la konservado de la neŭtraleco de la reto kaj la produktado de komunajo. Kvankam ĝi fine trovis sian vojon en la francan nacian juron, ĝi ne traktis la temon de amasa gvatado.¹³

En Germanio, ĵurnalisto, filozofoj (kiel ekzemple Jürgen Habermas) kaj politikistoj anoncis Ĉarton de Ciferecaj Rajtoj, sed la klopodo neniam sukcesis fariĝi nacie deviga leĝo.¹⁴

Dum Berners-Lee imagis iun formon de laŭleĝe deviga interkonsento inter la platformoj de Silicon Valley kaj nacio-ŝtatoj en la spirito de la originala Magna

Nemateria Konstitucio: La Post-Snowden-a Prizorgado de la Interreto

La interkonsento de Carta inter la ribelaj aristokratoj kaj la monarkio, la manko en la Interreto de iu ajn forumo kapabla realigi devigan leĝaron malfaciligis ĉi tiun taskon, kaj la fakto, ke la plej multaj nacio-ŝtatoj ne volis limigi la interretajn gvatagadojn de siaj propraj sekretaj servoj, malebligis la taskon. La diversaj provoj desegni aŭ kolekti retajn rajtojn restis nekoheraj kaj eĉ kontraŭdiraj (Redeker, Gill, kaj Gasser 2018): Kiel la rajto resti libera de reta misuzo, ekzemple, povas esti kongruigita kun la rajto je reta anonimeco? Klopodo, kiu laŭsupoze konduki al tutmonda revolucio en retaj rajtoj, la Magna Carta Iniciato estis lanĉita en 2015 sub la slogano "Reto, Kiun Ni Volas" fare de la Web Foundation, sekvante la ekzemplon de ĝia fondinto Berners-Lee. La Magna Carta por la TTT malfortiĝis, estante transdonita al Consumers International, fariĝante homamas-fonta kampanjo celita al junuloj en 2015 fare de la Brita Biblioteko por proponi kaj diskuti liston de dek ĉefaj retrajtoj.¹⁵ Fine en 2019, "Kontrakto por la TTT" gvidata de la Web Foundation estis aprobita de pli ol cent kvindek civilaj sociaj organizaĵoj, inkluzive de platformoj kiel Facebook, Microsoft, Amazon kaj Google. Tamen, la Kontrakto por la TTT ne estis laŭleĝe deviga.¹⁶ Tial, ĝi ne fakte haltigis gvatadon kaj celitan reklamadon, kiel abunde montris kreskanta nombro da skandaloj ĉirkaŭ la ĉiam pli misuzata konduto de registaroj kaj platformoj (Alibhai-Brown 2019). Kvankam bonintencaj, ĉi tiuj klopodoj estis malproksimaj de sufiĉaj por restarigi fidon je la Interreto. La realmonda efiko de amasgvatado ilustras kiel la intencoj de la originalaj dizajnistoj de teknologio povas malpli kaj malpli gravi laŭlonge de la tempo, ĉar tiuj intencoj per si mem - kiom ajn noblaj - ne malhelpis difektojn en la deplojo de la teknika sistemo mem, kiuj malobservis la akcepteblecon de la teknologio inter ĝiaj uzantoj.

Kvankam la inventinto de teknologio eble havas socian vizion pri la mondo, kiun ilia teknologio supozeble realigos, tiu vizio ne nepre estas garantiita per la realigo de ilia teknologio laŭlonge de la tempo. Berners-Lee imagis mondon de malfermaj datumoj kaj scio-interŝanĝo, tamen la ĉieesteco de la Reto ankaŭ kreis mondon de gvatado kaj sensekureco. Responde, Berners-Lee esperis, ke li povus, pro sia konsiderinda staturo kiel "inventinto" de la Reto, apelacii al politikaj procezoj por interveni en la estonteco de la teknologio, kiun li helpis desegni, sed Berners-Lee mem ne kapablis artiki sian propran vizion pri retaj rajtoj kaj tiel konstrui la necesan politikan forton por devigi tiun vizion. Dungita en la gvatado-komerco fare de Google, Cerf argumentis por pli konservativa interpreto de rajtoj kaj malakceptis ajnan reguligan intervenon por subteni retajn rajtojn en la Interreto.

Tamen, la malsukceso de kaj Cerf kaj Berners-Lee preni sekurecon kaj privatecon

Techné: Esplorado en Filozofio kaj Teknologio

konsideri dum la dizajnado de la Interreto kaj la TTT estas ĝuste tio, kio kondukis al cifereca amasa gvatado, kaj nek el ili povis solvi la krizon de fido al la Interreto, kiu rezultis. Konsiderante la malsukceson de la nobla provo de Berners-Lee krei internacian movadon por leĝdoni la misuzojn malkaŝitajn de Snowden, la tasko restarigi privatecajn rajtojn al la Interreto tiam falis al tiuj malpli konataj inĝenieroj ĉe la IETF laborantaj pri Interreta bontenado.

6. La Kripta Riparo de la Interreto

Plonĝi en la detalojn de la bontenado de IETF ilustras kiel ŝanĝi kaj aldoni novajn ecojn al teknika sistemo per la praktiko de riparo povas rekonstrui fidon inter la homoj, kiuj uzas ĝin. Restarigi fidon en la Interreto ŝajnis esti neebla tasko al Berners-Lee; la nesolvebla problemo ĉe la kerno de antaŭvidi ajnan konstitucion de la Interreto estas kiel devigi ĝin, konsiderante la jam menciitajn fiaskojn de naciaj registaroj kaj la mankon de tutmonda socia movado. Kiam Snowden deklaris sursceneje kun Berners-Lee, ke "Magna Carta por la Interreto estas ĝuste tio, kion ni bezonas: ni bezonas ĉifri niajn valorojn ne nur skribe sed ankaŭ en la strukturo de la Interreto", li provizis decidan komprenon pri kiel transiri de formala konstitucio bazita sur nura teksto al materia konstitucio.

bazita sur kodo kiu subtenas aron de ankoraŭ nedifinitaj retaj rajtoj (Pitts-Brooke 2014).

Skribita en natura lingvo, formala konstitucio estas dokumento kiu deklaras diversajn rajtojn kaj limigojn al suvereneco, dum materia konstitucio estas aparato de devigo, "historie determinita kaj historie kaŭzita punkto de kontakto inter rajto kaj fakto, kaj inter la jura organizado de potenco kaj ĝia socia strukturo" (Negri 1994, 63). La fakta konstitucio de la Interreto povas esti komprenata ne kiel skriba formala konstitucio kiu difinas rajtojn kaj respondecojn, sed prefere kiel teknikaj normoj kiuj difinas la ecojn kaj kapablojn donitajn de protokolo al uzantoj. Do anstataŭ skriba "Kontrakto por la Reto", estis ĉi tiuj fortikaj teknikaj ecoj, kiel sekreteco kaj privateco subtenataj de kriptografio, kiujn aldonis la IETF, kiuj pruviĝis decidaj por malhelpi gvatadon kaj restarigi fidon en la Interreto. Eĉ se oni konsideras protokolojn kaj kodon kiel negravajn, la operacioj de la protokolo formas la materian konstitucion de la Interreto.

Simile al diversaj juraj aliroj skizitaj antaŭe, unu provo de la IETF trakti la dizajnadon de protokoloj por konservi homajn rajtojn, kaj eble novajn retraĵtojn, estis krei Homrajtan Protokolon pri Konsideroj (HRPC).

Esplorgrupo, kies celo estis establi etikan revizion rilate al homaj rajtoj por iu ajn nova proponita IETF-normo (Mueller kaj Badiei 2019). Tamen,

Nemateria Konstitucio: La Post-Snowden-a Prizorgado de la Interreto

La HRPC malsukcesis starigi tian procezon por IETF-normoj kaj havis malfacilaĵojn mapi protokolkarakterizaĵojn al homaj rajtoj. Estis neniu deziro flanke de la inĝenieroj en la IETF provi devigi rajtojn, kiuj ne povus esti teknike artikulitaj, aŭ efektivigi koncepton de rajtoj, kiun ili konsideris deveni de ne-teknikaj fakuloj. La HRPC vekis zorgojn de inĝenieroj, ke devigi homajn rajtojn kiel donitajn de Unuiĝintaj Nacioj postulus superrigardon de ŝtatoj, kio estis anatemo por neŝtata normiga instanco, kiu ne havis aŭ volis oficialan juran statuson; kvankam ankoraŭ ekzistanta, la HRPC falis en sensignifecon ene de la IETF.

Anstataŭe, IETF decidis redukti kompleksan politikan problemon al pure teknika problemo, kiu povus esti solvita per inĝenierado; ilia respondo al amasa gvatado estis sekvi la sugeston de Snowden devigi la rajton je privateco per ebligado de moderna kriptografio laŭ la spirito de la maksimumo de Lawrence Lessig, ke "kodo estas leĝo" (1999), tasko pli facile kompletigebla ol okupiĝi pri filozofiaj debatoj pri difinado de novaj specoj de rajtoj. Baldaŭ post la revelacioj de Snowden, la inĝenieroj de IETF provis difini la naturon de la problemo per verkado de nova RFC titolita "Penetra Monitorado estas Atako" (RFC 7258), en kiu ili nomis amasan gvatadon "atako kontraŭ la privateco de retuzantoj kaj organizoj" (Farrell kaj Tschofenig 2014). En diskuto kun IETF-inĝenieroj ĉe IETF-kunveno en 2015, Snowden esprimis sian deziron, ke Interretaj protokoloj estu konscie ĝisdatigitaj por malhelpi amasan gvatadon.¹⁷ Certe, ekzistis larĝbaza interkonsento de la IETF, ke ĉiu uzanto de la Interreto meritas havi siajn komunikadojn protektitajn kontraŭ amasa gvatado fare de korporacioj (kiuj ofte estis la dungantoj de IETF-inĝenieroj!) same kiel registaroj. Kun ĉi tiu celo, kriptografiaj teknikoj estis uzitaj por certigi, ke "la dezajno de protokoloj" igas gvatadon "signife pli multekosta aŭ nefarebla" (Farrell kaj Tschofenig 2014, 1). Tiel, la inĝenieroj intuicie esprimis, konforme al Berners-Lee, novan specon de reta rajto al privateco, kiu iris preter tradiciaj homaj rajtoj.

Dum la NSA-likoj, la vasta plimulto de la interreta trafiko estis neĉifrita, kaj tial estis bagatela tasko por la NSA kapti kaj registri plejparton de la interreta trafiko per la gvatado de kelkaj Interretaj Interŝanĝaj Punktoj (IXP-oj). Ĉifrado inter la klientaj aparatoj de uzantoj kaj retejoj estis farita per IETF-normo nomata Transport Layer Security (TLS). Bedaŭrinde, la antaŭ-Snowden-versio de ĉi tiu normo, TLS 1.2, estis origine desegnita de amatoroj kaj tial malfermita al multaj atakoj (Adrian et al. 2015). Krome, ĉifrado per TLS ne estis deplojita, ĉar ĝi postulis, ke retejoj aĉetu multekostajn ciferecajn atestilojn de kompanioj.

Techné: Esplorado en Filozofio kaj Teknologio

por ĉifri retejan trafikon. La IETF decidis, ke la riparado de TLS por ĉifri la plimulton de la Interreto provizus la plej mallongan vojon al restarigo de fido en la Interreto.

Antaŭ la Snowden-revelacioj, la IETF havis sufiĉe komfortan rilaton kun la NSA. Konsiderante la amplekson de ilia perfido de sekurecaj normoj, kiel malkaŝite de la Snowden-revelacioj, estis alvoko forigi NSA-dungiton, Kevin Igoe, kiel kunprezidanton de la grava CryptoForum Research Group en 2014. Kvankam la alvoko por lia tuja forigo malsukcesis, li estis fine anstataŭigita per pli neŭtrala akademia kriptografo post la fino de lia oficperiodo. Jam en 2014, oni komencis laboron por ripari la TLS-protokolon por certigi ĝian sekurecon, precipe por ebligi la uzon de ne-NIST-aprobitaj elipsaj kurboj. Elipsa kurba kriptografio estis la plej rapida metodo por krei ĉifritan kanalon inter kliento kaj servilo en la TTT, sed la specifaj elipsaj kurboj, kiel la vaste uzata p-256-kurbo proponita de NIST, havis kelkajn misterajn parametrojn donitajn de la NSA, kvankam oni konsideris neverŝajne, ke ili estis kaŝitaj per malantaŭa pordo (Koblitz kaj Menezes 2016). La kriptografiisto Daniel J. Bernstein, kiu antaŭe persone procesis la usonan registaron por establi la juran precedencon en Usono laŭ la principo "kodo estas libera parolo", kiu permesas publikan aliron al kriptografia kodo, kreis eĉ pli rapidan alternativon al la NIST-kurboj, bazitan sur la publike produktita kaj kolege reviziita kurbo Curve25519 (Bernstein 2006). Konsiderante la plibonigojn de rapideco kaj la fidon generitan ĉe la IETF per akademia kolega revizio, ŝajnis tute nature, ke Curve25519 estu parto de TLS, malgraŭ manko de aprobo de NIST. Tamen, male al la normoj de AES kaj SHA, la NIST-kurboj ne estis produktitaj per la kutimaj publikaj konkursoj de NIST, kiu ankoraŭ havis konsiderindan fidon ene de la akademia normkomunumo. Por konservi fidon post-Snowden, la IETF tial inversigis sian tradician fluon de kriptografia normigado for de la NSA kaj NIST, fokusante anstataŭe sur kriptografiaj primitivoj de la akademia komunumo, kies malferma kulturo de kolega revizio nun estis konsiderata tre taŭga por la normiga procezo de IETF.

En tiu ĉi senco, la TLS IETF Laborgrupo estis revivigita en 2014 por permesi al TLS uzi neregistarajn aprobitajn elipsajn kurbojn. Eminentaj akademianoj aliĝis al la IETF-inĝenieroj por igi la specifojn multe pli rigoraj, uzante formalan konfirmon por pruvi la ecojn de TLS-efektivigoj kontraŭ ankoraŭ nekonataj atakoj, kvankam izolite de ilia pli vasta socia uzado (Bhargavan, Blan-chet, kaj Kobeissi 2017). Kvankam oni suspektus, ke la formaleco de IETF-specifoj kondukus ilin pli for de la realmonda praktiko, la pliigita uzo de pli precize difinitaj protokoloj fare de IETF-specifoj permesis pli bonan interrilaton.

Nemateria Konstitucio: La Post-Snowden-a Prizorgado de la Interreto

funkciadon de kodo kaj provizis gradon da certeco pri ilia sekureco. Novaj privatecaj funkcioj estis aldonitaj por malhelpi trafikanalizon de kontraŭuloj kiel la NSA, inkluzive de ĉifrado de pli granda parto de la komenca konekto inter klientoj kaj la TTT kaj ebligado de antaŭensekretado, tiel ke eĉ se ŝlosilo estus kompromitita, ĝi ne povus simple deĉifri la tutan konekton. La nova versio de TLS 1.3 estis vaste konsiderata vaste supera al antaŭaj TLS-versioj, kaj estis rapide adoptita de ĉiuj gravaj retumiloj.¹⁸ TLS ankaŭ estis rapide adoptita de multaj retejoj: Du dungitoj de Mozilo - delongaj IETF-volontuloj Eric Rescorla kaj John Aas

-
elpensis la ideon krei TLS-atestilojn senpage kaj kreis neprofitcelan organizaĵon por administri servilon nomatan "Let's Encrypt" por ilia distribuo. La procezo de ilia sekura kreado estis prezentita al IETF kiel la proponita normo ACME (Auto-matic Certificate Management Environment) en 2015 kiel RFC 8555.¹⁹ Antaŭ septembro, la unua versio de la RFC estis redaktita kaj la servilo "Let's Encrypt" kreis pli ol 300 milionojn da atestiloj, igante la plimulton de la interreta trafiko ĉifrita per TLS (Holz et al. 2020).

Ĉi tiu devigo de privateco per kodo okazis kontraŭ la volo de Berners-Lee, kiu esprimis opozicion al TLS, argumentante, ke anstataŭigi "http" per "https" rompus ekzistantajn ligilojn en la TTT.²⁰ Tamen, ĉi tiu argumento falis sur surdajn orelojn. Dum la inventintoj de la Interreto kaj la TTT ne povis konsenti pri kreado de nova laŭjure cifereca konstitucio por la Interreto, per sia ordinara laboro en la ombroj la IETF-inĝenieroj sukcesis devigi ĉifradon tra interretaj protokoloj, garantii la novan retan rajton al privateco de komunikado kaj tiel kreis faktan konstitucion por funkciigi kodon.

Teknologio — eĉ se ekigita de iu originala dezajno — ŝanĝiĝas laŭlonge de la tempo, ne nur responde al konkreta uzado sed ankaŭ al la sociaj atendoj de ĝiaj uzantoj. Kvankam ordinara homoj malĝustaj estis pri la teknika realo de la privateco donita al ilia ĉiutaga interreta komunikado, la plej multaj ne atendis esti kaptitaj en reto de amasa gvatado, kiel montras la publika kolero pri la NSA, kiu aperis de aktoroj tiel diversaj kiel la financministro de Germanio ĝis indiĝenaj sociaj movadoj en Sudameriko (Snowden 2019). Rilate al tio, la aldono de kriptografio al la Interreto fare de la IETF por konservi privatecon estis provo igi la Interreton denove plenumi la kriteriojn de publika akceptebleco, ripari la originalan nesekuran dezajnon por konformigi ĝiajn teknikajn operaciojn al la atendoj de ĝiaj uzantoj.

Techné: Explorado en Filozofio kaj Teknologio

7. Politikaj Konsekvencoj

La normiga dimensio de teknika normigo devas esti komprenita el la vidpunkto de politika filozofio. Notindas kiom radikala ĉi tiu respondo al la amasa gvatado de NSA fare de IETF estis esence, ĉar la deplojo de ĉifrado devigas certan absolutisman normigan argumenton kontraŭ gvatado.

Ĉi tiu iniciato baziĝis sur la neartikulacia ideologio de inĝenieroj, anstataŭ tradicia aliro bazita sur proporcieco rilate al la rajtoj de la nacio-ŝtato. Zorgoj, ke absoluta rajto al anonimeco ebligis novajn specojn de nerimarkebla krimado en la Interreto, kondukis al alvokoj de agentejoj kiel la FBI por malhelpi la Interreton "mallumiĝi".²¹ Tamen, oni konsideris neeble efektiviĝi malantaŭan pordon en kriptografian protokolon, kiu povus esti uzata nur per nacio-ŝtata aliro (Diffie kaj Landau 2007). Kvankam ŝajnas, ke la filozofia kadro de retaj rajtoj pledita de Berners-Lee estis finfine dividita de la inĝenieroj de la IETF, ironie estis la metodaro de Cerf - por kiu novaj kapabloj estis la respondeco de normigaj instancoj anstataŭ reguligo - kiu ebligis al la IETF devigi sian koncepton pri retaj rajtoj per teknika dekreto, sukcesa puĉo de grupo de mem-elektitaj inĝenieroj fronte al la plej potenca nacio-ŝtato en la mondo.

Ĉi tio malkaŝas, ke la IETF, kaj la teknikaj normigaj instancoj ĝenerale, ne nur estas fonto de teknika potenco, sed posedas specon de politika potenco antaŭe rezervita de la nacio-ŝtato (Lessig 1999). Anstataŭ koncepti la IETF kiel konstitucian instancon, kiel donas nacio-ŝtatoj kaj internaciaj instancoj kiel la ITU, estas pli bone koncepti la IETF kiel formon de konstituiga potenco, kiu ekzercas sian potencon per la normiga procezo anstataŭ per jura konstitucia kreado. Kiel Michael Hardt kaj Antonio Negri (2017) rimarkas, historie konstituiga potenco "emis izoli politikajn dinamikojn de ekonomiaj kaj sociaj bezonoj kaj traduki ilin en jurisdikciajn povojn de formala konstitucio".

(2017, 16). En la epoko de la Interreto, la konsistiga potenco "disvolviĝis per kontinuaj operacioj de renovigo daŭrigitaj en sinsekvaj konstituciaj iniciatoj - procezo kiu tenas malfermitaj la kunlaborajn konfliktajn dinamikojn" (Hardt kaj Negri 2017, 34). Prefere ol la kreado de pure formala konstitucio kiel la antaŭvidita Magna Carta por la Reto, la bontenado kaj riparado de teknikaj normoj servas kiel konstante evoluanta "nemateria" konstitucio bazita sur la malfermaj asembleoj kreitaj per la normiga procezo de la IETF. La ironio estas, ke la abstraktaj principoj de retaj rajtoj donitaj en nemateria konstitucio estas materiaj-

Nemateria Konstitucio: La Post-Snowden-a Prizorgado de la Interreto

igite per protokoloj deplojitaj al miliardoj da uzantoj, operacio multe pli efika ol ankoraŭ plia deklaro de malplenaj vortoj.

Ekzistas fundamenta ligo inter teknika bontenado kaj rajtoj, kiu fine povas esti eksplicita, kiu iras preter la speciala kazo de la Interreto kaj povus esti konsiderata parto de pli granda filozofia malakcepto de transcendentata nocio de rajtoj. La kadro de homaj rajtoj estis kreita sub Klumisma koncepto pri la homo, kiu limigis kognajn kapablojn al tiuj naturigitaj kiel biologie enecaj en la individuo. Kiam kognaj kapabloj ene de la kapo, kiel ekzemple memoro, estas subkontraktitaj al la Interreto kiel parto de pli vasta procezo de distribuita pensado, la demando pri rajtoj nature devus konsideri la Interreton. Konsideru la averaĝan retuzanton kaj fabriklaboriston en la deknaŭa jarcento: La fabriklaboristo devas trakti mondon de muntlinioj kaj laborhoroj, dum la retuzanto traktas mondon de retejoj kaj artefarita inteligenteco; malgraŭ havi la saman specon de fizika cerbo, ili havas tre malsamajn specojn de mensoj. El ĉi tiu perspektivo, ne ekzistas transcendentata nocio de rajtoj, kiu estas iel sendependa de historio kaj teknologio; rajtoj devas konsideri la historiajn kondiĉojn kaj ŝanĝiĝi kiam tiuj kondiĉoj ŝanĝiĝas. Revenante al la ekzemplo de fabrika laboro: La kadro de leĝoj, kiu protektis homojn antaŭ la apero de organizita industria laboro, estis tre malsama ol la kadro, kiu rezultis el la laborluktoj de la 18-a kaj 19-a jarcentoj. Fabriklaboristo povis batali por rajtoj ĉirkaŭ laborhoroj, ĉar la koncepto de "labortago" ekzistis same kiel la rajto al privata vivo ekster la laboro, koncepto kiu ne ekzistis por la mezepoka kamparano. Same kiel la rajtoj de la antaŭindustria farmisto devis esti radikale ŝanĝitaj pro industriigo, kadro de rajtoj konstruita ĉirkaŭ subjekto, kies identeco estas interplektita en translima cifereca teknologio, devas konsideri la Interreton. La nemateria konstitucio faras ĉi tiujn...

retaj rajtoj estas nemalhaveblaj por ĉiuj uzantoj de la Interreto, senescepte — kaj tial estas je iu nivelo malpli hipokrita ol formala konstitucio, kiu simple deklaras transcendentajn rajtojn, sed praktike faras sennombrajn esceptojn per ne doni egalajn rajtojn al malplimulto aŭ permesi al suverena potenco funkcii senpune kontraŭ tiuj etikeditaj kiel "teroristoj" kaj "necivitanoj" (Agamben 2005). Tamen malgraŭ ĝiaj avantaĝoj, la racia ordigo de rajtoj en nemateria konstitucio estas nekonata, kaj tie kuŝas danĝero.

La kunfandiĝo de teknika kaj politika potenco en la Interreto abundas je eblecoj por revivigi certajn utopiajn demokratajn idealojn pri rajtoj kaj samtempe sanktigi novajn formojn de teknologia tiraneco per kodo. Kvankam la bontenado de la Interreto povas esti konsiderata kiel konstituiga procezo, kiu estas kaj demokratia kaj

Techné: Esplorado en Filozofio kaj Teknologio

teknika, ĝi ne estas absolute demokratia. Fine, la IETF estas finfine mem-elektita asembleo de inĝenieroj, devenantaj ĉefe el Usono kaj la grandaj kapitalismaj firmaoj de Silicon Valley kun tre malmulta partopreno de la faktaj uzantoj de la Interreto, inkluzive de la vasta plimulto de la monda loĝantaro en la Tutmonda Sudo (Halpin 2013). Provoj post la Snowden-revelacioj krei formon de Interreta regado, kiu metas la Tutmondan Sudon en la centron, kiel ekzemple la NetMundial-Iniciato gvidata de Brazilo, estis fine detruitaj de usonaj interesoj, inkluzive de la IETF. Ekzemploj kiel ĉi tiu sugestas la originan ideon de Berners-Lee, ke pli vasta, de malsupre supren, socia movado eble finfine necesas por transformi la Interreton en vere demokratian spacon. Negri asertas, ke rajtoj baziĝas sur konflikto, kaj kodo ne povas frostigi la substajn sociajn antagonismojn: "La fundamento de rajto estas la ŝanĝebleco, la artikulacio, kaj la konstante nova konfiguracio de la konflikteco" (1994, 101).

Pri tio, puĉo kontraŭ la IETF mem okazas: Nova generacio de inĝenieroj, kun Snowden, Manning kaj Assange ĉiuj subtenantaj, provas restrukturi demokratian kaj malcentralizitan Interreton preter Silicon Valley, bazitan sur enskribo de kaj retaj rajtoj - kaj posedrajtoj - en kodon per blokĉena teknologio (De Filippi kaj Wright 2018). Normoj ankaŭ ne estas la sola maniero protekti la rajton al privateco, kaj novaj protokoloj povas esti konstruitaj ekster iu ajn normo fare de korporacioj. Ekzemple, neprofitcelaj organizaĵoj kaj noventreprenoj laboras pri miksretoj, kiuj konstruas supermetaĵan reton sur la ekzistanta Interreto, kiu ne nur ĉifras, sed ankaŭ "miksas" Interretajn pakafetojn kune por malhelpi kontraŭulojn kiel la NSA determini la metadatenojn, kiel la tempigon kaj volumenon de pakafetoj, enecajn en TCP/IP-pakafeta dissendo (Diaz, Halpin, kaj Kiayias 2021). Tamen, la demando pri kiel la Interreto povus esti regata, kaj teknike konservata, kiel rekta demokratio implikanta ĝiajn miliardojn da uzantoj restas nesolvita.

8. Konkludo

La kolektiva bontenado de la Interreto fare de la IETF spite al amasa gvatado estas kazesploro pri la povo de la teknikaj spertuloj kanalogi popularajn postulojn en teknologian ŝanĝon eĉ spite al opozicio de nacio-ŝtatoj. Por resumi nian argumenton: Unue, ni ekzamenis diferencojn en kiel oni povas aliri retajn rajtojn kiel privateco en la Interreto, kiel montrite de la debato inter Berners-Lee kaj Cerf. Poste ni esploris kiel la Interreto povas esti difinita abstrakte per kolekto de teknikaj normoj por protokoloj kaj montris kiel normoj konvenas en la pejzaĝon de komputilaj protokoloj kaj programoj. Rilate al bontenado, la IETF ilustras kiel la malferma funkciado de la Interreto...

Nemateria Konstitucio: La Post-Snowden-a Prizorgado de la Interreto

dependas de la reagoj inter normoj, efektivigoj kaj uzantoj. Per la deplojo de ĉifrado tra siaj normoj responde al la populara kolero, la IETF rekonstruis fidon en la Interreto fronte al tio, kio ŝajnis esti amasa malobservo de rajtoj kaŭzita de la NSA. Kiom longe ĉi tiu fido daŭros en la estonteco, konsiderante la centraligon de la Interreto en malgrandan manplendon da usonaj entreprenaj platformoj kaj la riskon de ĝia fragmentiĝo pro cenzuro kaj kontrolo, restas malferma demando.

La ĉefa punkto de ĉi tiu verko estas, ke prizorgado povas transformi teknologion responde al desube supren politika premo, punkto aplikebla al vasta gamo da teknologioj preter la Interreto. Fumnebulon unue estis rimarkita de dommastrinoj en Beverly Hills, kio kondukis al protestoj kaj lobiado, kiuj igis la ŝtaton Kalifornio krei pli striktajn aŭtomobilajn normojn limigantajn karbonan poluadon, kaj nur per ĝeneraligita premo la konstruita medio kaj publika transporto fariĝis alireblaj por tiuj kun certaj handicapoj; ĉi tiuj ŝanĝoj en nia ĉiutaga teknika infrastrukturo nun povas esti konsiderataj memkompreneblaj, sed en ĉi tiuj intervenoj kuŝas la kerno de potenca praktiko, kiu povus esti esenca en nia teknologia mondo konsiderante la disvolviĝantajn tutmondajn krizojn kiel klimata ŝanĝo (Feen-berg 2017).

Esenca kontribuo de la nuna studo estas provizi filozofian analizon pri la rolo de normoj, kun fokuso aparte sur normoj en komputiko, ĉar ĝi estas ofte preteratentata aspekto de la reproduktado de teknologioj post ilia komenca produktado. La filozofia analizo de normoj povus esti utila por vasta gamo da teknikaj sistemoj, de la metra sistemo ĝis ISO-normoj por nutraĵsekureco. Kiel ekzempligite per la kazo de la IETF, malferma kontribuo al demokratiaj normigaj procezoj, kontraste al tradicia desupra procezo de burokratia normigado, povus esti unu maniero trakti la daŭrajn zorgojn pri novaj teknologioj kiel AI, kie la problemoj de gvato kaj privateco denove provokas protestegon kaj instigas vokojn por novaj internaciaj normoj (Lewis et al. 2020). Normigado povas esti vidata kiel avenuo por demokratia interveno en teknologian disvolviĝon, kiu malfermas tion, kion Herbert Marcuse nomis "la traduko de valoroj en teknikajn taskojn" (1964, 232).

Fine, ni montris kiel la intencoj de la inventinto(j) de teknologio povas esti superitaj de decidoj faritaj dum la laboro de bontonado, kiel ekzemple montras la politikaj debatoj substantaj la daŭran disvolviĝon de Interretaj normoj post la rivelacioj de Snowden. Riparo ne estas nur restarigo de teknologio al origine celita dezajno kaj povas esti komprenata kiel inkluzivanta la kreivan kaj politikan laboron de ŝanĝo de teknika funkciado por kongrui kun ŝanĝiĝantaj sociaj kriterioj de akceptebleco, irante konsiderinde preter la intencoj de la inventintoj per...

Techné: Esplorado en Filozofio kaj Teknologio

procezo de kontestado kaj intertraktado inter teknikaj fakuloj kaj la publiko.

Dum la argumento de Cerf, ke finfine respondecas pri la Interreto teknikaj normigaj instancoj, anstataŭ tradiciaj leĝdonaj instancoj, montriĝis ĝusta, lia pozicio, ke la Interreto ne devus impliki homajn rajtojn, estis kontraŭdirita de la argumento de Berners-Lee por la rekono de novaj fundamentaj retaj rajtoj rilate al privateco (2012), kiujn fine devigitaj de la IETF per la ĝeneraligita deplojo de normoj por cifrado. La fakto, ke IETF-inĝenieroj ankaŭ laboris ĉe kompanioj kiel Google, kiuj ankaŭ povis deploji ĉi tiujn normojn sen longaj leĝdonaj procezoj, sendube estis faktoro en ilia sukceso.

Ĉi tio elstarigas punkton, kiun preteratentis la aserto, ke teknikaj spertuloj mediacias popularan zorgon pri teknologioj kaj tial ŝanĝas ilin laŭ politika premo pri novaj kriterioj de akceptebleco, kiujn atentigas la ne-teknikaj masoj (Feenberg 2017). Teknikaj spertuloj povas formi sian propran klason kun siaj propraj interesoj en la koro, kaj tiel agi en la nomo de la uzantoj de teknologio sen provizi al ili ian ajn senchavan demokratian reprezenton, kiel jam antaŭe vidis en kazoj tiel diversaj kiel Sovetunio kaj Silicon Valley. En ekzemplo, kie teknika normigo determinis politikon, la prizorgantoj de la Interreto kaj reprezentis sed ankaŭ saltis antaŭ la uzantoj de sia teknologio, kiam la IETF decidis devigi senkondiĉan privatecon per kodo por venki la amasajn gvatadajn povojn de nacio-ŝtatoj. Plia filozofia esplorado estas necesa por determini la valentojn de ĉi tiu aŭdaca daŭranta movado de inĝenieroj por sublimigi la socian en la teknikan.

Agnoskoj

Ĉi tiu artikolo estas dediĉita al la memoro de Antonio Negri, kiu inspiris mian unuan verkon pri la politiko de la Interreto en la revuo *Multitudes*. Toni rivelis, ke la kreiva povo de la homamaso estas la ofte neagnoskita motoro de politiko, tezo, kiun mi modeste plivastigas por kovri la Interreton.

Nemateria Konstitucio: La Post-Snowden-a Prizorgado de la Interreto

Notoj

1. La Reto temas pri la universala transportado de datumoj tra retoj, dum la TTT estas difinita per universala nomsistemo konstruita sur la Reto, ĉefe uzata en hiperteksto (Halpin 2008).

2. <https://www.itu.int/rec/T-REC-X.200-199407-1>

3. <https://www.ietf.org/rfc/rfc1122.txt>

4. <https://www.ietf.org/rfc/rfc1123.txt>

5. <https://www.ietf.org/rfc/rfc1.txt>

6. <https://www.ietf.org/rfc/rfc675.txt>

7. La detaloj pri la funkciado de la IETF estis priskribitaj pli detale el la vidpunkto de filozofio (Halpin 2008), antropologio (Ten Oever 2021), kaj historio (Abbate 1999).

8. <https://www.ietf.org/rfc/rfc3986.txt>

9. <https://www.w3.org>

10. <https://www.rfc-editor.org/rfc/rfc8713>

11. <https://www.cgi.br/pagina/marco-civil-law-of-the-internet-in-brazil/180>

12. https://www.camera.it/application/xmanager/projects/leg17/commissione_internet/testo_definitivo_inglese.pdf

13. Leĝo n-ro 2016-1321 de la 7-a de oktobro 2016 por Cifereca Respubliko.

14. <https://digitalcharta.eu/>

15. <https://www.bbc.com/news/technology-33132662>

16. <https://contractfortheweb.org/>

17. <https://www.internetsociety.org/blog/2015/07/edward-snowden-elstaraĵoj-identeco-kaj-privateco-ĉe-ietf-93/>

18. <https://www.ietf.org/rfc/rfc8446>

19. <https://www.ietf.org/rfc/rfc8738.html>

20. <https://www.w3.org/DesignIssues/Security-NotTheS.html>

21. <https://archives.fbi.gov/archives/news/speeches/going-dark-are-teknologia-privateco-kaj-publika-sekureco-sur-kolizia-kurso>

Referencoj

Abbate, Janet. 1999. Inventante la Interreton. Kembriĝo: MIT Press.

Adrian, David, Karthikeyan Bhargavan, Zakir Durumeric, Pierrick Gaudry, Matthew Green, J.

Alex Halderman, Nadia Heninger, Drew Springall, Emmanuel Thom, Luke Valenta,

Benjamin VanderSloot, Eric Wustrow, Santiago Zanella-Béguelink, kaj Paul Zimmermann.

2015. "Neperfekta Antaŭen-Sekreteco: Kiel Diffie-Hellman Malsukcesas en Praktiko." En

Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications

Security, 5–17. Denver, Usono. Novjorko: ACM Press. [https://doi.org/](https://doi.org/10.1145/2810103.2813707)

10.1145/2810103.2813707

- Agamben, Giorgio. 2005. *Stato de Escepto*. Ĉikago: Universitato de Ĉikago Eldonejo.
<https://doi.org/10.2307/j.ctv1134d6w.16>
- Alibhai-Brown, Yasmin. 2019. "La nova 'kontrakto por la reto' estas nur bona PR por la teĥnologiaj megalomaniuloj, kiuj daŭre faros sian plej malbonan." *La gazeto I*, 25-a de novembro 2019.
<https://inews.co.uk/opinion/contract-web-tim-berners-lee-facebook-microsoft-google-367231>.
- Appelbaum, Jacob. 2022. *Komunikado en Mondo de Pervasiva Gvatado*. Doktora disertaĵo. Eindhoven, Nederlando: Teknologa Universitato de Eindhoven.
- Aristotelo. 1924. *La Metafiziko de Aristotelo Volumo II*, trad. William David Ross. Oksfordo: Clarendon Press. <https://doi.org/10.1093/actrade/9780198847779.book.1>
- Baran, Paul. 1964. *Pri Distribuitaj Komunikadoj*. Vaŝingtono: RAND-Raporto Serio. <https://doi.org/10.7249/RM3766>
- Berners-Lee, Tim, kaj Harry Halpin. 2012. "Defendu la Reton." En *Digital Enlightenment Yearbook*, red. Jacques Bus, Michael Crompton, Mireille Hildebrandt, kaj George Metakides, 3–7. Amsterdamo: IOS Press. <https://doi.org/10.3233/978-1-61499-057-4-3>
- Bernstein, Daniel. 2006. "Curve25519: Novaj Diffie-Hellman-rapidecaj rekordoj." En *Internacia Konferenco pri Teorio kaj Praktiko en Publikŝlosila Kriptografio*, 207–28. Novjorko, Usono. Berlino: Springer. https://doi.org/10.1007/11745853_14
- Bhargavan, Karthikeyan, Bruno Blanchet, kaj Nadim Kobeissi. 2017. "Konfirmitaj Modeloj kaj Referencaj Efektivigoj por la Normo-Kandidato TLS 1.3." En *2017 IEEE Simpozio pri Sekureco kaj Privateco*, 483–502. San-Francisko, Usono. Piscataway: IEEE-eldonejo. <https://doi.org/10.1109/SP.2017.26>
- Boriso, Alexandre, Emanuelle Reynaud, François Osiurak, kaj Jordan Navarro. 2018. "Akcepto- kaj akcepteblo-kriterioj: Literatura recenzo." *Kognado, Teknologio kaj Laboro* 20(2): 165–77. <https://doi.org/10.1007/s10111-018-0459-1>
- Cerf, Vinton. 2012. "Aliro al Interreto ne estas homa rajto." *New York Times*. 4-a de januaro 2012: 25–26. <https://doi.org/10.1109/TCOM.1974.1092259>
- Cerf, Vinton, kaj Robert Kahn. 1974. "Protokolo por Paketa Reta Interkomunikado." *IEEE Transactions on Communications* 22(5): 637–48.
- Clark, Andy, kaj David Chalmers. 1998. "La Plilongigita Menso." *Analizo* 58(1): 7–19. <https://doi.org/10.1093/analys/58.1.7>
- Clark, David. 2018. *Dezajnante Interreton*. Kembriĝo: MIT Press. <https://doi.org/10.7551/mitpress/11373.001.0001>
- De Filippi, Primavera, kaj Aaron Wright. 2018. *Blokĉeno kaj la Juro: La Regulo de Kodo*. Kembriĝo, Masaĉuseco: Harvard University Press. <https://doi.org/10.4159/9780674985933>
- Diaz, Claudia, Harry Halpin, kaj Aggelos Kiayias. 2021. *La Reto Nym: La Sekva Generacio de Privateca Infrastrukturo*. <https://nymtech.net/nym-whitepaper.pdf>.

Nemateria Konstitucio: La Post-Snowden-a Prizorgado de la Interreto

- Diffie, Whitfield kaj Martin Hellman. 1976. "Novaj Direktoj en Kriptografio." *IEEE Transactions on Information Theory* 22(6): 644–54. <https://doi.org/10.1109/TIT.1976.1055638>
- Diffie, Whitfield, kaj Susan Landau. 2007. *Privateco en risko: La politiko de subaŭskultado kaj ĉifrado*. Kembriĝo: MIT Press. <https://doi.org/10.7551/mitpress/5572.001.0001>
- Farrell, Stephen kaj Hannes Tschofenig. 2014. "Penetra Monitorado estas Atako." IETF RFC 7258. <https://www.ietf.org/rfc/rfc7258.txt>. <https://doi.org/10.17487/rfc7258>
- Feenberg, Andrew. 2017. *Teknosistemo: La Socia Vivo de Racio*. Kembriĝo: Harvard University Press. <https://doi.org/10.4159/9780674982109>
- Halpin, Harry. 2008. "La Nemateria Aristokratario de la Interreto." *Mute* 2(8): 98–120.
- Halpin, Harry. 2013. "Senmateria Civita Milito: La Tutmonda Milito en la Reto." *Culture Machine* 14(1): 1–24.
- Hardt, Michael, kaj Antonio Negri. 2017. *Asembleo*. Oksfordo: Oxford University Press.
- Koblitz, Neal, kaj Alfred Menezes. 2016. "Enigmo envolvita en enigmo." *IEEE Security & Privacy* 14(6): 34–42. <https://doi.org/10.1109/MSP.2016.120>
- LaRue, Frank. 2011. Raporto de la Speciala Raportisto pri la antaŭenigo kaj protekto de la rajto je libereco de opinio kaj esprimo. Ĝenerala Asembleo de Unuiĝintaj Nacioj. https://www.ohchr.org/sites/default/files/english/bodies/hrcouncil/docs/17-a_sesio/A.HRC.17.27_eo.pdf.
- Lessig, Lawrence. 1999. *Kodo kaj Aliaj Leĝoj de Ciberspaco*. Novjorko: Bazaj Libroj.
- Lewis, Dave, Linda Hogan, David Filip, kaj Patrick Wall. 2020. "Tutmondaj defioj en la normigo de etiko por fidinda AI." *Journal of ICT Standardization (Ĵurnalo de IKT-Normigado)* 8(2): 123–50. <https://doi.org/10.13052/jicts2245-800X.823>
- Leyden, John. 2014. "Vint Cerf volis igi la Interreton sekura ekde la komenco, sed sekreteco malhelpis ĝin." *The Register* 7-a de aprilo 2014. https://www.theregister.com/2014/04/07/internet_inception_security_vint_cerf_google_hangout/.
- Licklider, Joseph. 1963. "Memorando por Membroj kaj Filioj de la Intergalaksia Komputila Reto." ARPA-Memorando 23-a de aprilo 1963. <https://www.ibiblio.org/hhalpin/dokumentoj/intergalaksia.pdf>.
- Linebaugh, Peter. 2009. *La Manifesto de Magna Carta: Liberecoj kaj Komunaj por Ĉiuj*. Berkeley: Universitato de Kalifornio. <https://doi.org/10.1525/9780520932708>
- Marcuse, Herbert. 1964. *Unu-Dimensia Homo: Studoj pri la Ideologio de Progresinta Industria Societo*. Bostono: Beacon Press.
- Monnin, Alexandre, kaj Harry Halpin. 2012. "Direkte al filozofio de la reto: fundamentoj kaj malfermaj problemoj." *Metaphilosophy* 43(4): 361–79. <https://doi.org/10.1111/j.1467-9973.2012.01764.x>

Techné: Esplorado en Filozofio kaj Teknologio

- Mornin, Joseph. 2014. "NSA Metadatena Kolekto kaj la Kvara Amendo." *Berkeley Technology Law Journal* 29(1): 985–1006.
- Mueller, Milton, kaj Farzaneh Badieli. 2019. "Rekviemo por Revo: Pri Antaŭenigo de Homaj Rajtoj per Interreta Arkitekturo." *Politiko kaj Interreto* 11(1): 61–83. <https://doi.org/10.1002/poi3.190>
- Negri, Antonio. 1994. "Laboro en la Konstitucio." En *Laboro de Dionizo*, red. Michael Hardt kaj Antonio Negri, 53–135. Minneapolis: Universitato de Minesoto-Gazetaro.
- Palermos, Spyridon Orestis. 2023. "Datumoj, Metadatenoj, Mensaj Datumoj? Privateco kaj la Plivastigita Menso." *AJOB Neuroscience* 14(2): 84–96. <https://doi.org/10.1080/21507740.2022.2148772>
- Pitts-Brooke, Jack. 2014. "Tim Berners-Lee aliĝas al Edward Snowden sursceneje por virtuala altkvin-babilado kaj privata babilado." *The Independent* Marto 2014. <https://www.independent.co.uk/tech/tim-bernerslee-aliĝas-al-edward-snowden-scene-por-virtuala-babilado-pri-malaltiĝo-kaj-privateco-9203165.html>.
- Redeker, Dennis, Lex Gill, kaj Urs Gasser. 2018. "Direkte al Cifereca Konstituciismo?" *Mapante Provojn Krei Interretan Deklaracion de Rajtoj.* *Internacia Komunikada Gazeto* 80(4): 302–319. <https://doi.org/10.1177/1748048518757121>
- Smart, Nigel. 2016. *Kriptografio Simpligita*. Berlino: Springer. <https://doi.org/10.1007/978-3-319-21936-3>
- Smart, Paul. 2017. "Etendita Kogno kaj la Interreto: Revizio de Aktualaj Temoj kaj Kontroversioj." *Filozofio kaj Teknologio* 30(3): 357–90. <https://doi.org/10.1007/s13347-016-0250-2>
- Snowden, Edward. 2019. *Permanenta Rekordo: Memorajo de Malvolonta Denuncanto*. Novjorko: Macmillan.
- Solove, Robert. 2008. *Komprenante Privatecon*. Kembriĝo: Harvard University Press.
- Ten Oever, Niels. 2021. "'Ĉi Tio Ne Estas Kiel Ni Imagis Ĝin': Teknologiaj Affordancoj, Ekonomiaj Faktoroj, kaj la Imago de Interreta Arkitekturo." *Novaj Amaskomunikiloj kaj Socio* 23(2): 344–62. <https://doi.org/10.1177/1461444820929320>
- Winner, Langdon. 2014 [1983]. "Teknologioj kiel Formoj de Vivo." En *Etiko kaj Aperantaj Teknologioj*, red. Ronald L. Sandler, 48–60. Londono: Palgrave Macmillan. https://doi.org/10.1057/9781137349088_4
- Wittgenstein, Ludwig. 1953. *Filozofiaj Esploroj*. Oksfordo: Wiley Blackwell.
- Wittgenstein, Ludwig. 1969. *Pri Certeco*. Oksfordo: Wiley Blackwell.
- Yates, JoAnne, kaj Craig Murphy. 2019. *Inĝenieraj Reguloj: Tutmonda Normo-Fiksado ekde 1880*. Baltimoro: John Hopkins University Press.
- Young, Mark Thomas. 2020. "Prizorgado." En *La Routledge Manlibro de la Filozofio de Inĝenierarto*, red. Diane Michelfelder kaj Neelke Doorn, 356–68. Novjorko: Routledge.
- Zittrain, Jonathan. 2008. *La Estonteco de la Interreto: Kaj Kiel Haltigi Ĝin*. New Haven: Yale University Press.