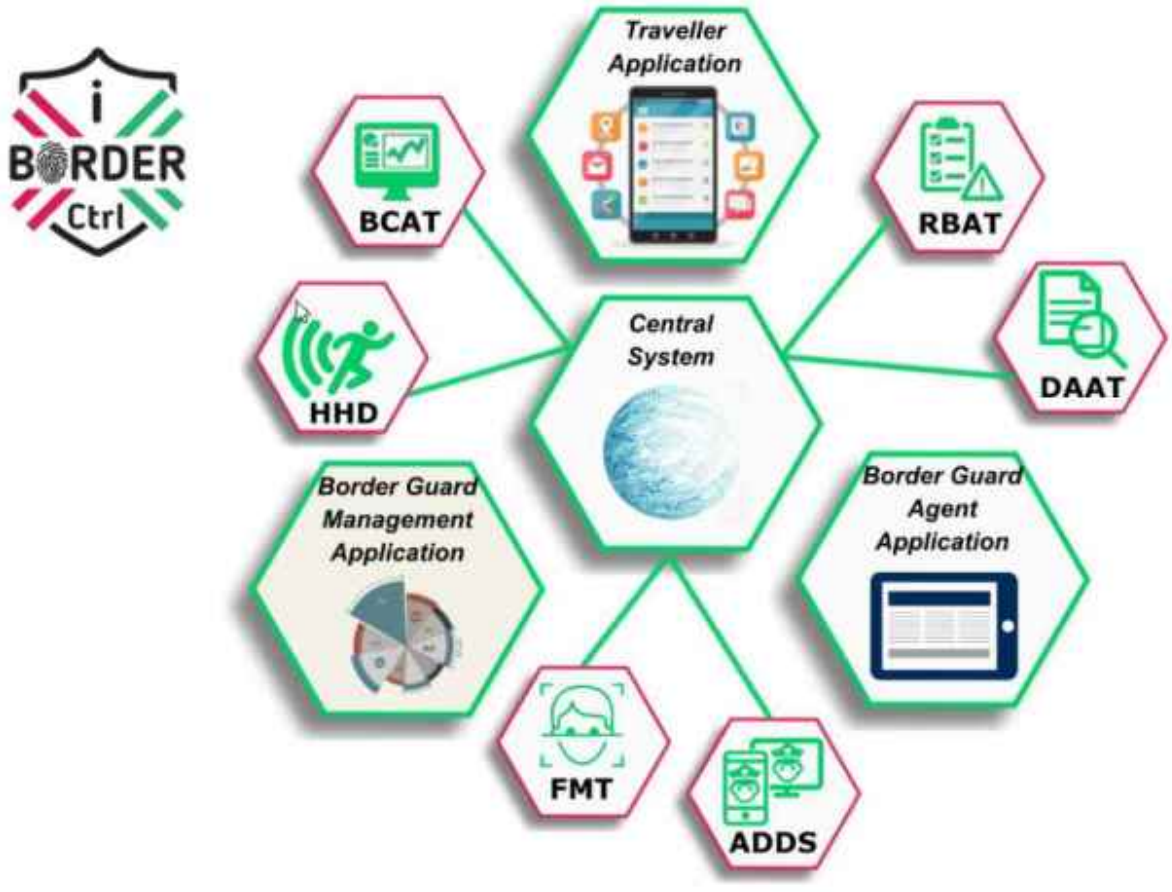
door Matthias Monroy (*)
1 mei 2021
Overgenomen van Globalinfo
dat zorgde voor de vertaling van het oorspronkelijk artikel

Drie jaar lang heeft een consortium van Europese bedrijven, instituten, universiteiten en politiediensten in een EU-project gewerkt aan technologieën om het werk van grens- en douaneautoriteiten te vergemakkelijken. Verschillende toepassingen werden gecombineerd in een "intelligent draagbaar grenscontrolesysteem" (iBorderCtrl), dat ambtenaren via een mobiel apparaat kunnen raadplegen. Het principe is dat reizigers zoveel mogelijk persoonlijke gegevens zelf in het systeem invoeren voordat zij het land binnenkomen.

Het platform voert vervolgens een risicobeoordeling uit en betrekt daarbij andere gegevensbronnen. Een algoritme beslist of de persoon als ongevaarlijk wordt geclassificeerd. Daarna kan de grensovergang bij automatische controlepoorten snel en soepel verlopen. Wie door iBorderCtrl als risicovol wordt aangemerkt, moet een "handmatige" grenscontrole doorlopen.



Kortere uitgebreide controles

Met onderzoek zoals iBorderCtrl wil de EU-Commissie het probleem oplossen dat de controles aan de buitengrenzen van de EU vanaf 2023 aanzienlijk langer zullen duren. Aanleiding is de invoering van een "Entry/Exit System" (EES), waarbij ook reizigers uit visumvrije landen een gezichtsopname en vier vingerafdrukken moeten afgeven. Tot nu toe was dit alleen nodig voor een visum of een asielaanvraag.

Voor het EES zullen alle grensovergangen te land, ter zee en op luchthavens worden uitgerust met apparatuur voor het afnemen van biometrische gegevens. Voorts zal worden geïnvesteerd in zelfbedieningskiosken waar reizigers hun gezichtsopname en vingerafdrukken kunnen laten aflezen van de RFID-chip van hun paspoort. Als het paspoort niet biometrisch is, kan de machine de nodige beelden zelf nemen.

Analyses van microgedragingen

Een centraal onderdeel van iBorderCtrl is een virtuele grenswacht die reizigers een tiental vragen stelt en nagaat of zij een "positieve" indruk maken. Ook dit wordt meegenomen in de risicobeoordeling. Dergelijke "misleidingsdetectie" door een politieavatar kan bij de grensovergang plaatsvinden, maar ook van tevoren.

Dit kan nuttig zijn voor een "reisinformatie- en machtigingssysteem" (ETIAS), dat de Europese Unie in 2023 in gebruik zal nemen. Reizen moeten dan worden aangekondigd voordat zij de grens overschrijden. Frontex zal verantwoordelijk zijn voor de daaropvolgende risicoanalyse van de voorziene reizigers aan de hand van een "watch list". Daarbij zou het grensagentschap ook gebruik kunnen maken van "misleidingsdetectie".

Frontex financiert sinds 2009 onderzoek aan de universiteit van Arizona, waarbij de nauwkeurigheid van een Automatic Deception Detection System (ADDS) wordt geëvalueerd. Hiernaar werd verwezen in iBorderCtrl. Het daar gesimuleerde verhoor vond plaats in het kader van een preregistratie, zoals voorzien in ETIAS. Reizigers zouden daarvoor de webcam van hun computer of mobiele toestel moeten gebruiken.

De ADDS kwantificeert de waarschijnlijkheid van bedrog door de zogenaamde microgedragingen van de respondenten te analyseren. Het systeem stelt vervolgens een statistische waarschijnlijkheid vast van "bedrieglijk gedrag" van de reizigers. De EU-richtlijn inzake rechtshandhaving verbiedt geautomatiseerde besluitvorming, dus een dergelijke beoordeling moet door een grenswacht worden geverifieerd.

Presentatie aan Frontex

Omdat de procedures die in de ADDS worden getest als een “leugendetector” werken, heeft het EU-project hevige kritiek gekregen. In reactie daarop hebben de betrokkenen en de EU-Commissie verzekerd dat het alleen om onderzoek gaat en dat er geen plannen zijn om “bedriegerdetectie” in te voeren in de grenscontrolesystemen van de EU. Deze geruststelling is echter in twijfel getrokken nadat europarlementariër Patrick Breyer een bewerkt document van iBorderCtrl weer leesbaar wist te maken.

Het iBorderCtrl-project werd geleid door het Europese IT-bedrijf European Dynamics. Uit het nu niet-gecensureerde document blijkt dat het bedrijf de projectresultaten bij Frontex in Warschau heeft gepresenteerd. Verdere presentaties zouden plaatsvinden tijdens “conferenties, tentoonstellingen, evenementen en workshops”. Andere projectpartners kondigden aan dat zij individuele modules aan hun nationale grensautoriteiten zouden presenteren, maar ook in verdere Frontex-workshops.

De Manchester Metropolitan University, die ook betrokken is en op wiens 20 jaar oude “Silent Talker”-machine de onderzochte “bedriegerdetectie” is gebaseerd, was van plan deze te presenteren op het Wereldcongres over Computationele Intelligentie. Soortgelijke beloften werden gedaan door de Leibniz Universität Hannover, die het begeleidende ethische onderzoek in iBorderCtrl heeft verricht. Hiervoor zouden de blog en de sociale-mediakanalen van de universiteit worden gebruikt.

Angst voor publiek debat

Het is waarschijnlijk niet ongebruikelijk dat onderzoekers aan het eind van een EU-project hun resultaten ophemelen en verdere promotie beloven. De EU-Commissie heeft tenslotte de volledige kosten van 4,5 miljoen euro betaald. Uit de bewerkte delen van het document blijkt echter dat wetswijzigingen bedoeld waren om momenteel verboden technologieën in te voeren.

Om de resultaten van iBorderCtrl “doeltreffend” in de bestaande grenscontrolesystemen te integreren, kunnen volgens het document “enkele politieke en juridische hervormingen nodig zijn”. Het gaat daarbij om “misleidingsdetectie”, maar ook om de geautomatiseerde analyse van Twitter-accounts van reizigers. Daarom, aldus het document, is het “belangrijk dat de resultaten van het project worden verspreid onder de beleidsmakers op EU- en nationaal niveau”.

Daartoe wordt voorgesteld dat “de voornaamste belanghebbenden naar behoren moeten worden aangesproken”. Leden van nationale parlementen en EU-parlementariërs worden genoemd als besluitvormers, evenals de Europese Commissie, politie- en grensautoriteiten en relevante ministeries. Ten slotte, als derde groep, moeten “de burgers” voor de nieuwe bewakingstechnieken worden gewonnen. De makers van IBorderCtrl verwachten geen “duidelijke consensus”. Zij voeren zelfs aan dat een controversieel openbaar debat “de uitvoering van het voor iBorderCtrl vereiste beleid zou kunnen belemmeren”.

“Lobby voor wetswijzigingen”

De scepsis over iBorderCtrl wordt nog versterkt door het feit dat essentiële details over de technische werking van de afzonderlijke toepassingen geheim worden gehouden. Patrick Breyer, die voor de Piratenpartij in het Brusselse parlement zit, heeft hiertegen juridische stappen ondernomen bij het Europese Hof van Justitie (HvJ) in Luxemburg. Na een hoorzitting in februari wacht het parlementslid nu op een uitspraak die openbaar toezicht op de Europese onderzoeksfinanciering mogelijk maakt.

Breyer is dan ook geschokt door de onthullingen van het niet-geredigeerde document en bekritiseert “dat EU-onderzoeksfondsen in feite worden gebruikt om te lobbyen voor wetswijzigingen die onze grondrechten beknotten”.

Dit geldt vermoedelijk ook voor een ander project waarin het onderzoek dat in 2019 met iBorderCtrl werd beëindigd, zal worden voortgezet. Een “Technology-supported Risk Estimation by Predictive Assessment of Socio-technical Security” (TRESPASS) heeft tot doel grenscontrole- en douaneautoriteiten te voorzien van “risicogebaseerde profilering” om “smokkel, illegale immigratie, grensoverschrijdende criminaliteit en terrorisme” op te sporen en te vervolgen. In tegenstelling tot iBorderCtrl heeft de Commissie haar financiering voor TRESSPASS zelfs bijna verdubbeld tot ongeveer 8 miljoen euro.

“Beoordeel de oprechtheid van de reiziger”

Ook in TRESSPASS wordt de vooraf door reizigers verstrekte informatie gecorreleerd, gevolgd door een bevraging van de sociale media en het “dark web”. Als mensen vervolgens op de luchthaven aankomen, worden ze geobserveerd door een “real-time gedragsanalyse”. Reizigers en hun bagage kunnen daartoe met scanners worden gescreend. TRESSPASS gaat ook verder dan iBorderCtrl wat betreft de databanken die voor de risicoanalyse worden gebruikt.

Op de website van het project antwoordt TRESSPASS op de vraag of ook “leugendetectoren” worden onderzocht met “Ja, in algemene zin”. Als een verdachte reiziger wordt ondervraagd, kan de technologie “nuttig zijn om specifiek opgeleide grenswachten te helpen de oprechtheid van de reiziger en zijn verklaringen sneller en nauwkeuriger te beoordelen”.

(*) Matthias Monroy is kenniswerker, activist, redacteur van het Duitse burgerrechtentijdschrift Bürgerrechte & Polizei (CILIP)