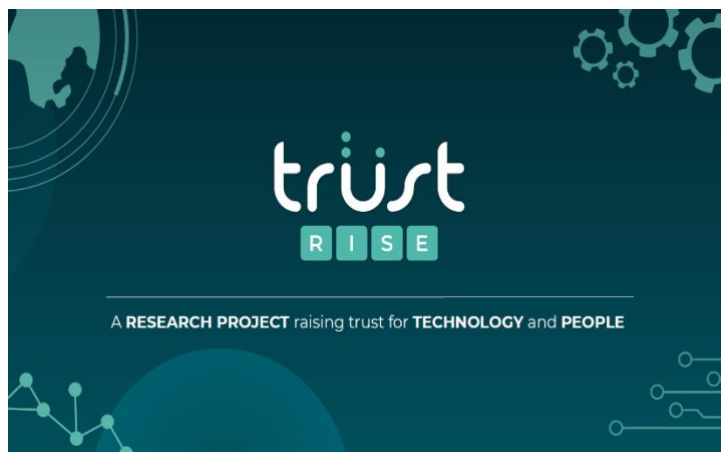




TRUST - digital TuRn in EUrope: Strengthening relational reliance through Technology

**De digitale revolutie. Nieuwe dimensies van vertrouwen,
bescherming van fundamentele rechten, en uitdagingen voor
hedendaagse rechtssystemen**

Beleidsadvies

Massimo Meccarelli (UniMc), Francesco Gambino (UniMc), Rafael del Asis Roig (UC3M), Ermanno Calzolaio (UniMc), Laura Vagni (UniMc), Oscar Celador Angon (UC3M), Andrea Raffaele Amato (UniMc), Elena Codoni (UniMc), Chiara Comberiati (UniMc), Alessandra Dignani (UniMc), Gabriel Faustino Santos (UniMc), Jacopo Fortuna (UniMc), Ludovica Ilari (UniMc), Chiara Iorio (UniMc), Beatrice Lupacchini (UniMc), Giorgia Vulpiani (UniMc)

Vertaling: Geert Deconinck (KU Leuven)



This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under grant agreement n. 101007820.

This document reflects only the author's view. The Research Executive Agency is not responsible for any use that may be made of the information it contains

De digitale revolutie. Nieuwe dimensies van vertrouwen, bescherming van fundamentele rechten, en uitdagingen voor hedendaagse rechtssystemen

De **digitale verandering** toont op steeds relevantere wijze een buitengewoon innovatief potentieel wat betreft de impact op het leven van mensen, en krijgt een steeds grotere betekenis voor rechtssystemen en hun traditionele categorieën. Een van de uitdagingen van het **TRUST-project: digital TuRn in EUrope: Strengthening relational reliance through Technology**, bestaat uit het onderzoeken van de nieuwe dimensies van vertrouwen die voortvloeien uit de technologische en digitale verschuiving, met inachtneming van de impact ervan op juridische veranderingen en de dynamiek van aanpassing.

Om dit doel te bereiken – vanuit methodologisch perspectief – moeten twee relevante aspecten in overweging worden genomen, die een beter begrip van het onderzochte fenomeen mogelijk maken en waardevolle axiologische aanknopingspunten bieden voor het oplossen van de problemen die voortkomen uit de vergelijking tussen traditionele rechtssystemen en nieuwe innovatieve digitale instrumenten.

- Het eerste aspect betreft de **tijdregimes** die inherent zijn aan het innovatieverschijnsel zelf. Nieuwe digitale technologieën volgen namelijk transformatietijden die niet in lijn liggen met die van de juridische dimensie. Het gaat niet alleen om de snelheid waarmee ze worden gerealiseerd, maar ook om de houding ten opzichte van verandering die de technologische sfeer onderscheidt van de juridische. Terwijl **technologie** noodzakelijkerwijs gericht is op voortdurende verbetering (**dynamiek / transformatie**), neigt **het recht** er daarentegen toe om, om zijn ontologische functie te vervullen, statische configuraties te behouden (**onveranderlijkheid / stabiliteit / weerbaarheid**).
- Het tweede aspect betreft de **transdisciplinaire dimensie** van het probleem. De digitale verschuiving lijkt namelijk niet vanuit één enkel perspectief – het strikt juridische – analyseerbaar, maar vereist noodzakelijkerwijs de betrokkenheid van verschillende kennisbronnen, afkomstig uit diverse rechtsgebieden (publiek, privaat, internationaal, administratief, enz.) en uit sectoren zoals informatica, economie, ethiek en geschiedenis, dewelke beleidsmakers en juristen niet zonder kunnen. Het is uiteraard een proces dat zijn structurele effecten pas op lange termijn zal kunnen uitdrukken – waarvan de uitkomsten moeilijk (zo niet onmogelijk) te voorspellen zijn – maar dat desalniettemin niet benaderd kan worden zonder rekening te houden met zijn intrinsieke interdisciplinariteit.

Door deze twee aspecten te combineren, hebben we geprobeerd – vanuit een juridisch perspectief dat openstaat voor het begrijpen van de specificiteit van technologische instrumenten en hun functionaliteiten – de belangrijkste innovaties te onderzoeken die verband houden met de introductie van **blockchain (blokketens)** en **nieuwe digitale technologieën** in het dagelijks leven van hun gebruikers (mensen, bedrijven, instellingen, enz.). Beginnend bij het idee van een **gedecentraliseerd systeem** – met alle implicaties die dit met zich meebrengt op het gebied van privacy en consumentenbescherming – of het concept van **gedematerialiseerde goederen** of **instrumenten**, zoals NFT's, cryptovaluta of smart contracts, via het massale gebruik van op **AI** gebaseerde technologieën in ondernemings- of Europese interne marktcontexten, tot aan de ethische dilemma's die worden opgeworpen door computerhacking en **cybersecurity**. Daarbij wordt geprobeerd de compatibiliteit van deze nieuwe geavanceerde technologische instrumenten met de huidige

normatieve systemen (nationaal en supranationaal) te verifiëren en mogelijke oplossingen te schetsen (normatief, regulerend, doctrinair, jurisprudentieel of via *soft law*) die het mogelijk maken het dynamisme van technische innovatie – in voortdurende en onophoudelijke transformatie en implementatie – te verenigen met de weerbaarheid van het recht en zijn traditionele categorieën, die weinig geneigd zijn tot radicale verandering maar onvermijdelijk neigen naar aanpassing en transformatie, mits correct begrepen en zonder vooroordelen ten opzichte van de digitale revolutie.

De bescherming van rechten en vrijheden in het informatietijdperk: innovatieve uitdagingen en passende juridische oplossingen

Er zijn veel levensdomeinen waarin de opkomst van nieuwe technologieën – en in het bijzonder **blockchain** en andere **geavanceerde digitale hulpmiddelen** – een aanzienlijke impact hebben. Dit vereist dat rechtsstelsels zich aanpassen aan deze veranderingen om de **fundamentele rechten en vrijheden** van zowel **gebruikers** als van **uitvinders, producenten of leveranciers** beter te beschermen.

De relatie tussen recht en nieuwe technologieën is een thema dat zich geleidelijk heeft ontwikkeld en een belangrijke factor van maatschappelijk belang is geworden. Dit was al het geval bij de eerste technologische innovaties van de 19e eeuw – zoals spoorwegen, telegrafie, stoommachines, elektriciteit of de eerste verbrandingsmotoren – die het leven van honderdduizenden mensen in korte tijd ingrijpend veranderden. Het recht, met zijn normatieve functie, komt vaak in een crisis terecht bij technische vooruitgang en de uitvinding van instrumenten of diensten die het leven snel transformeren. Zijn onvermogen om zich snel aan te passen aan deze vooruitgang veroorzaakt een onevenwicht dat wetgevers en juristen uitdaagt om het bestaande regelgevingskader te herzien, verouderde categorieën te herdenken en instellingen en principes op een innovatieve manier te herinterpreteren, zodat het traditionele juridische denken zich kan aanpassen aan nieuwe, onvoorziene situaties en opkomende behoeften.

Toch lijkt de rol van het recht niet bedreigd, zelfs niet in deze crisismomenten. De centrale positie ervan blijft een belangrijke factor in het **bevorderen en ontwikkelen van vertrouwen** in nieuwe technologieën. Dit komt doordat de performatieve kracht van juridische instellingen (principes, categorieën, concepten, normatieve oplossingen, jurisprudentie, enz.) in staat is gebleken om conflicten die voortvloeien uit technologische implementatie op te lossen, en zo een adequaat kader te bieden voor de bescherming van het individu en diens fundamentele rechten.

Daarom moet de komst van de meest geavanceerde technologische hulpmiddelen rechtsstelsels ertoe aanzetten zich te vernieuwen, zonder zich af te sluiten – zonder vooruitgang te negeren of de innovatieve reikwijdte ervan te ontkennen. Het moet politiek en rechtswetenschap stimuleren om nieuwe soorten problemen op te lossen, en de best mogelijke oplossingen te vinden om technologische ontwikkeling adequaat te combineren met de persoonlijke en vermogensrechtelijke prerogatieven van het individu.

Kijkend naar de context van de Europese Unie en haar 27 lidstaten, kunnen er ten minste zeven belangrijke uitdagingen worden geïdentificeerd waarmee beleidsmakers en juridische interpretatoren vandaag de dag worden geconfronteerd om het gebruik van nieuwe technologieën in overeenstemming te brengen met de normen voor de bescherming van fundamentele rechten en vrijheden in de Europese ruimte. Hier zijn de zeven uitdagingen:

1. **Verzoenen van Verordening nr. 2016/679 (AVG / GDPR) met blockchaintechnologie**, zodat het gebruik ervan de rechten van gebruikers niet in gevaar brengt.
2. Implementeren van EU-regels over digitale hulpmiddelen om ze aan te passen aan nieuwe kwesties die voortvloeien uit de verspreiding van **kunstmatige intelligentie (AI)**.

3. Herschrijven van fundamentele categorieën van het privaatrecht om ze compatibel te maken met gedematerialiseerde activa zoals **NFT's** of **cryptovaluta**.
4. Herinterpreteren van fundamentele beginselen van het contractenrecht en die van de goede werking van de Europese markt, aangepast aan het gebruik van slimme instrumenten zoals **smart contracts**.
5. Oplossingen bedenken die ondernemingen beschermen tegen het gebruik van **geautomatiseerde procedures** die milieuduurzaamheid kunnen bedreigen of de juiste afweging van belangen kunnen verstoren.
6. Harmoniseren van regels inzake grondbezit om grootschalige toepassing van blockchain in **kadastrale digitalisering** mogelijk te maken.
7. Zorgvuldig beoordelen van het ethisch-juridische gewicht dat bepaalde **cybersecurity-instrumenten** kunnen hebben, om zo cyberdreigingen voor gegevensbeveiliging te beperken.

Blockchain en Verordening nr. 2016/679 (AVG / GDPR)

Een van de meest urgente kwesties voor het Europese rechtstelsel is ongetwijfeld de compatibiliteit tussen **Verordening (EU) nr. 2016/679 – de Algemene Verordening Gegevensbescherming (AVG / GDPR)** – en **blockchaintechnologie**. De grootste moeilijkheid ligt in het verzoenen van twee instrumenten – één regulerend (de GDPR) en de ander technologisch (blockchain) – die gebaseerd zijn op fundamenteel verschillende structurele kenmerken die op het eerste gezicht onverenigbaar lijken.

De GDPR is gebaseerd op een gecentraliseerd model met identificeerbare verwerkingsverantwoordelijken en verwerkers van persoonsgegevens, terwijl blockchain (vooral in zijn publieke, 'permissionless' vorm) gedecentraliseerd is en geen centrale controle kent. De GDPR werd ingevoerd vóór de brede verspreiding van blockchain, wat verklaart waarom deze niet ontworpen is om de uitdagingen van gedecentraliseerde technologieën aan te pakken.

Toch blijft de Europese verordening het fundamentele juridische kader dat uniforme bescherming van rechten met betrekking tot nieuwe technologieën binnen de EU garandeert, en blockchain moet zich daar noodzakelijkerwijs aan houden. De naleving van de GDPR door blockchain hangt meer af van de wijze waarop de technologie wordt toegepast dan van de technologie zelf. Dit verklaart waarom er geen eenduidige oplossing bestaat, maar dat deze afhangt van verschillende factoren die naar voren komen in specifieke gebruikssituaties.

Een van de belangrijkste zorgen is het identificeren van wie als **verwerkingsverantwoordelijke** kan worden beschouwd binnen een blockchainnetwerk, en hoe gebruikers hun rechten onder de GDPR kunnen uitoefenen. De grootste uitdaging is het vinden van een evenwicht tussen de bescherming van persoonsgegevens van gebruikers en de ontwikkeling en het gebruik van blockchain in overeenstemming met de regelgeving. Dit brengt aanzienlijke verplichtingen met zich mee voor verwerkingsverantwoordelijken – vooral in het geval van publieke blockchains – waar het identificeren van verantwoordelijken en het toepassen van de regelgeving een open vraag blijft.

Alleen specifieke regelgeving die rekening houdt met de bijzonderheden van blockchain en de vereisten van de GDPR aanpast aan verschillende gebruikssituaties, kan effectieve bescherming van de rechten van betrokkenen garanderen zonder het gebruik van blockchain te belemmeren.

In dit opzicht is een interessant experiment de regelluwe zone of **regulatory sandbox**, die terrein wint als oplossing voor de uitdagingen van regelgevingsinconsistentie bij **Distributed Ledger Technology (DLT)** of **gedistribueerde grootboektechnologieën**. Het doel van deze sandbox is om regelgevers en toezichthouders in staat te stellen samen te werken met vernieuwers, best practices

te delen en hun begrip van blockchaintechnologieën te verbeteren binnen een pan-Europees regelgevend kader.

De **European Blockchain Regulatory Sandbox** – gepromoot door de Europese Commissie in het kader van het Digital Europe-programma – beoogt een veilige regelgevingsomgeving te creëren om het gebruik van deze technologie te testen en beter te reguleren. Hoewel het pad niet zonder obstakels is, lijkt de mogelijkheid om Europese “gouden standaarden” voor blockchain te creëren die als referentie kunnen dienen voor andere rechtsgebieden wereldwijd, veelbelovend.

Naast deze kwesties over de werking van het blockchainnetwerk en de implicaties ervan voor de bescherming van individuele rechten in de EU, voorziet de GDPR ook in strikte controles op de overdracht van persoonsgegevens buiten de Europese Economische Ruimte (EER). Dienstverleners moeten ervoor zorgen dat dergelijke gegevens alleen worden overgedragen aan landen met een passend beschermingsniveau volgens EU-normen. Dit is bijzonder uitdagend in een publieke blockchain, waar gegevens worden gerepliceerd over alle knooppunten, ongeacht hun geografische locatie.

Een van de belangrijkste innovaties van de GDPR is dat de naleving ervan niet beperkt is tot Europese landen, maar zich uitstrekt tot elke entiteit die goederen of diensten aanbiedt in de Europese Unie, ongeacht of deze Europees is of niet. Alle personen en bedrijven die actief zijn in de EU zijn verantwoordelijk voor de verwerking van persoonsgegevens in hun bezit, moeten voldoen aan verschillende regels met betrekking tot gegevensbeveiliging en moeten een functionaris voor gegevensbescherming aanstellen, met mogelijk zware sancties bij niet-naleving.

Zelfs als gegevens in de blockchain kunnen worden versleuteld of gepseudonimiseerd, is het vaak mogelijk om personen achter transacties opnieuw te identificeren, wat het recht op anonimiteit – zoals gegarandeerd door de GDPR – kan schenden.

Kunstmatige Intelligentie (AI)

Naast het opleggen van normen voor de bescherming van persoonsgegevens in blockchain (Verordening (EU) nr. 2016/679 (GDPR)), streeft deze er ook naar om een uniform juridisch kader te creëren voor de ontwikkeling, het gebruik en de implementatie van **kunstmatige intelligentie (AI - artificial intelligence)**-systemen binnen de Europese Unie.

Het belangrijkste doel is ervoor te zorgen dat AI mensgericht, betrouwbaar en veilig in gebruik is, gericht op het respecteren en beschermen van de fundamentele rechten van individuen (zoals privacy, gezondheid, veiligheid, enz.) en vrij van misbruik of manipulatie door derden. In dit opzicht bevordert de GDPR technologische innovatie en beschermt zij consumenten tegen oneerlijke praktijken.

Om dit te bereiken, definieert de Europese wetgeving verschillende sleutelbegrippen, zoals:

- **"AI-systeem"** – elk systeem dat in staat is om voorspellingen, aanbevelingen of beslissingen te nemen met verschillende graden van autonomie;
- **"Biometrische gegevens"** en **"emotieherkenning"**, waarvan het gebruik wordt gereguleerd om ethische en privacyproblemen te voorkomen.

Daarnaast verplicht de GDPR **"verantwoordelijke partijen"** of **"aanbieders"** – gedefinieerd als degenen die dergelijke systemen ontwikkelen of op de markt brengen – om ervoor te zorgen dat hun producten voldoen aan de Europese normen. Dit omvat voortdurende conformiteitsbeoordelingen en toezicht na de ingebruikname van de systemen.

De verordening voorziet ook in specifieke toestemmingsvereisten voor **"gevoelige contexten"**, evenals een duidelijk kader voor toezicht in geval van datalekken. Het is aan nationale en EU-toezichthoudende autoriteiten om ervoor te zorgen dat het gebruik van AI voldoet aan de hoogste

ethische en veiligheidsnormen, zodat gebruikers worden beschermd tegen misbruik door dienstverleners of exploitanten.

NFT's en Cryptovaluta

Een ander zeer actueel onderwerp betreft **non-fungible tokens (NFT's)** en **cryptovaluta**, die een aanzienlijke uitdaging vormen voor traditionele juridische categorieën.

Momenteel blijven de intellectuele eigendomsrechten met betrekking tot NFT's onduidelijk. De aankoop van een NFT betekent niet automatisch dat de onderliggende intellectuele eigendomsrechten worden overgedragen, tenzij dit expliciet is vermeld. Juridische discussies suggereren dat bestaande intellectuele eigendoms wetten – waaronder auteursrechten en merkenrechten – van toepassing zijn op NFT's.

Naarmate de NFT-markt blijft groeien, zullen juridische kwesties met betrekking tot auteursrechten, geregistreerde merken en de bescherming van digitale kunst waarschijnlijk aanzienlijk evolueren. Kunstenaars en makers zullen hun praktijken mogelijk moeten aanpassen aan zowel traditionele als digitale beschermingsmechanismen, terwijl rechtsstelsels zich moeten blijven aanpassen aan de specifieke uitdagingen die NFT's met zich meebrengen. Daarbij moet worden verduidelijkt of NFT's autonome kunstwerken zijn of slechts digitale representaties van bestaande intellectuele eigendom.

Deze vaststelling leidt onvermijdelijk tot de vraag naar **civiele aansprakelijkheid** met betrekking tot de creatie en circulatie van NFT's. In Italië wordt Distributed Ledger Technology (DLT) en smart contracts momenteel geregeld via artikel 8-ter van Wet 12/2019. Deze bepaling definieert DLT in brede zin, maar behandelt NFT's niet specifiek.

Op supranationaal niveau sluit **Verordening (EU) nr. 2023/1114 – de Markets in Crypto-Assets Regulation (MiCAR)** – NFT's uit van haar toepassingsgebied en richt zich in plaats daarvan op *fungibele* cryptovaluta. Deze regelgevende leemte betekent dat geschillen met betrekking tot NFT's moeten worden opgelost op basis van algemene beginselen van contracten- en eigendomsrecht.

Gezien de diversiteit van NFT's kan hun juridische behandeling een **casus-per-casusanalyse** vereisen. Sommige NFT's, zoals die welke financiële producten vertegenwoordigen, kunnen onder de effectenwetgeving vallen, terwijl andere eerder binnen het kader van eigendoms- of contractenrecht passen.

Een andere opkomende kwestie met betrekking tot NFT's – maar ook van toepassing op cryptovaluta – is hun **erfrechtelijke status**. Als digitale activa kunnen zowel NFT's als cryptovaluta in theorie worden opgenomen in testamenten of trusts. Een van de praktische uitdagingen is echter de toegang tot de privésleutels die nodig zijn om NFT's en cryptovaluta na overlijden over te dragen. Dit benadrukt het belang van **nalatenschapsplanning** die rekening houdt met digitale activa.

Een mogelijke oplossing om de overdracht van digitale activa te waarborgen is het model van de **digitale nalatenschap of wachtwoord-erfenis**, waarbij toegangsgegevens worden opgenomen in een testament of veilig worden opgeslagen voor de erfgenaam. In dit model fungeren de inloggegevens als een "sleutel" die toegang geeft tot digitale inhoud of activa, zoals NFT's of cryptovaluta.

Ondanks de groeiende bewustwording dat digitale activa deel kunnen uitmaken van een nalatenschap, zijn juridische innovaties en meer gedetailleerde oplossingen nodig om een soepele overdracht van deze activa te garanderen.

Blockchain en Smart Contracts

Binnen de context van de Europese interne markt stelt **blockchaintechnologie** ontwrichtende uitdagingen, aangezien zij het potentieel heeft om meerdere economische en juridische dynamieken te hertekenen, waaronder die welke worden gereguleerd door het Europese mededingingsrecht.

Het **Verdrag betreffende de werking van de Europese Unie (VWEU)** verbiedt overeenkomsten, besluiten van ondernemersverenigingen en onderling afgestemde gedragingen die tot doel of gevolg hebben de mededinging binnen de interne markt te beperken of te vervalsen. In dit opzicht kan blockchain verschillende rollen spelen. Enerzijds zou het een platform kunnen worden voor mededingingsbeperkende afspraken; anderzijds kan de inherente transparantie ervan dienen als een **compliance-instrument**, dat precieze traceerbaarheid van transacties mogelijk maakt en zo geheime samenspanning beperkt.

Aangezien de technologie gebaseerd is op gedeelde protocollen en consensusalgoritmen, zou zij theoretisch coördinatie tussen marktdeelnemers kunnen vergemakkelijken, bijvoorbeeld als knooppunten in het netwerk blockchain gebruiken om prijzen af te stemmen, markten te verdelen of strategische beslissingen te coördineren.

Een van de grootste praktische moeilijkheden bij de toepassing van het mededingingsrecht op blockchainnetwerken is de sterk gedecentraliseerde aard van de technologie, waardoor het moeilijk is om met zekerheid de verantwoordelijke(n) voor onrechtmatig gedrag te identificeren en dus te sanctioneren.

De Europese Commissie zal daarom interpretatieve criteria moeten ontwikkelen om deelname aan een blockchain te beoordelen, of specifieke regelgevende wijzigingen moeten overwegen om opkomende knelpunten aan te pakken. Mogelijke strategieën om de toepassing van het Europese recht effectiever te maken, zonder het potentieel van blockchain te onderdrukken, zijn onder meer:

- Versterking van de samenwerking tussen mededingingsautoriteiten en toezichthouders in de *fintech*- en digitale sectoren;
- Ontwikkeling van specifieke richtsnoeren voor de blockchainsector die als indicatoren kunnen dienen voor mogelijke samenspanning of misbruik van machtspositie;
- Gespecialiseerde opleidingen over blockchain voor personeel van mededingingsautoriteiten, markttoezichthouders en rechters, aangezien de analyse van mogelijke inbreuken niet alleen juridische expertise vereist, maar ook diepgaande kennis van gedistribueerde protocollen, consensusmechanismen, cryptografische methoden en gemeenschapsgebaseerde bestuursdynamieken.

Vanuit een meer civielrechtelijk perspectief – maar nog steeds gericht op het goed functioneren van de interne markt – kan het gebruik van **smart contracts** een aanzienlijke impact hebben, niet alleen op de naleving van mededingingsregels, maar ook op de correcte totstandkoming van de contractuele wil van individuele consumenten.

In dit verband rijst het delicate probleem van **defecten in toestemming (wilsgebreken)**, veroorzaakt door vergissingen, foutieve uitingen van contractuele wil of mogelijke computerfouten die het functioneren van het blockchainprotocol verstoren, waardoor de consument een aankoop doet die hij anders niet zou hebben gedaan.

Smart contracts – vanwege hun technische kenmerken en automatische uitvoering – vormen een aanzienlijk risico voor consumenten, aangezien de automatisch gegenereerde effecten (doorgaans onveranderlijk) het gevolg kunnen zijn van een systeemfout of ver verwijderd kunnen zijn van de werkelijke wil van de contractpartijen, waardoor deze vanaf het begin wordt gewijzigd of ongeldig worden.

Een mogelijke oplossing voor dit soort problemen is het aanpassen van traditionele civielrechtelijke regels aan de kenmerken van de nieuwe technologie, door een nieuwe theorie van dwaling en contractuele wil te ontwikkelen die rekening houdt met wat er in de digitale ruimte kan gebeuren.

Nieuwe technologieën en corporate governance

In de afgelopen decennia is het gebruik van nieuwe technologieën in de bedrijfspraktijk sterk toegenomen. Steeds meer ondernemingen maken gebruik van **kunstmatige intelligentie (AI)** om hun doelstellingen op het gebied van milieuduurzaamheid te verbeteren. Daarnaast kunnen digitale hulpmiddelen worden ingezet om communicatiekanalen met belanghebbenden te openen, informatiestromen te beheren en het bestuursorgaan te ondersteunen bij de naleving van recente Europese regelgeving.

Een van de innovatiegebieden betreft de automatisering van bedrijfsrapportage, die recent is geregeld via **Europese Richtlijn nr. 2022/2464**, beter bekend als de **Corporate Sustainability Reporting Directive (CSRD)**. AI-tools worden daadwerkelijk gebruikt om een rapportagesysteem te ondersteunen dat in staat is om de nodige informatie voor duurzaamheidsverplichtingen te verzamelen, verwerken en communiceren.

Bovendien biedt het gebruik van blockchaintechnologie en smart contracts – vooral voor grote digitale bedrijven – een kans om aandeelhouders en stakeholders te betrekken bij bedrijfsbeslissingen, en om te experimenteren met vormen van decentralisatie van besluitvormingsprocessen.

Toch kunnen veel van deze technologieën ook negatieve effecten hebben die in overweging moeten worden genomen. Hoewel ze waardevolle ondersteuning bieden bij het houden van virtuele aandeelhoudersvergaderingen – wat de betrokkenheid van aandeelhouders en stakeholders bij het management vergroot en de leidende rol van de algemene vergadering of de dialoog met institutionele investeerders versterkt – brengen ze ook risico's met zich mee.

Bijvoorbeeld: het gebruik van AI op basis van geavanceerde machine learning-algoritmen kan leiden tot **oneerlijke discriminatie** van stakeholders met gelijke verdiensten. Vanuit juridisch oogpunt is de belangrijkste kwestie het vaststellen van de **aansprakelijkheid van bestuurders** voor beslissingen die zijn genomen op basis van intelligente technologie, vooral wanneer de beoordelingen van het algoritme hebben geleid tot financiële, strategische of operationele keuzes die niet in overeenstemming zijn met het belang van de onderneming of met het nastreven van duurzaamheidsdoelstellingen.

Tot op heden bestaat er geen specifieke regelgeving op Europees niveau die dit fenomeen regelt. Toch kan worden gesteld dat het gebruik van algoritmen – hoewel het de optimalisatie van aanbevelingen en richtlijnen mogelijk maakt op basis van reeds vastgestelde management- en strategische doelstellingen – **niet op zichzelf in staat is om relevante belangen te selecteren en de noodzakelijke afwegingen te maken**. De uiteindelijke verantwoordelijkheid voor de koers van de onderneming blijft bij de bestuurders liggen.

Kadastrale digitalisering

De toepassing van **blockchaintechnologie** op **kadastrale registers** – zoals bij elke andere technologische innovatie – brengt onvermijdelijk zowel kansen als risico's met zich mee. Het is een traag en complex proces dat in alle landen van continentaal Europa afhankelijk is van de systemen die

worden gebruikt voor de overdracht van eigendomsrechten en van de functies die aan het kadaster zijn toegekend.

Zonder twijfel biedt blockchain een kans om de efficiëntie van bestaande kadastrale systemen te verbeteren, op voorwaarde dat er een adequate aanpassing en erkenning van de juridische relevantie van dit systeem plaatsvindt. In dit opzicht zijn er nog veel nationale rechtsstelsels die transacties die via blockchain worden uitgevoerd niet als legitiem beschouwen en dus niet als registreerbaar in het kadaster.

Een van de belangrijkste voorwaarden voor de toepassing van blockchaintechnologie op dit gebied is daarom de **harmonisatie van de regels die het registreren van eigendomsrechten regelen**. Deze harmonisatie zou het mogelijk maken om de bevolking van het Europese grondgebied te voorzien van instrumenten die de toegang tot kadastrale diensten vergemakkelijken, nuttige informatie over eigendomsregistratie binnen de Europese Unie beschikbaar maken en richtlijnen bieden voor een betere organisatie van kadastrale systemen in verschillende rechtsgebieden.

De ethiek van cybersecurity

Blockchaintechnologie is naar voren gekomen als een krachtig instrument om de complexe ethische en juridische uitdagingen aan te pakken die zich voordoen op het gebied van **cybersecurity**. De unieke kenmerken ervan – zoals decentralisatie, transparantie, cryptografie en onveranderlijkheid – hebben geleid tot veel belangstelling voor innovatieve oplossingen om cyberdreigingen te beperken.

In deze context kan blockchain worden beschouwd als een **sleutelstrategie** om ethische risico's te beperken, vertrouwen te versterken, gegevensintegriteit te waarborgen en verantwoordelijkheid te bevorderen in digitale transacties. Toch is blockchain op zichzelf niet voldoende om het volledige spectrum van ethische risico's in cybersecurity aan te pakken. Het moet worden geïntegreerd met andere benaderingen – zoals **kwantitatieve beoordelingen van ethisch risico** – die een gestructureerde methodologie bieden voor het evalueren en beperken van potentiële bedreigingen.

Door blockchaintechnologie te combineren met deze kwantitatieve beoordelingsmethoden kunnen organisaties een robuuster en ethisch verantwoord cybersecuritykader opbouwen. Om het potentieel van blockchain in cybersecurity maximaal te benutten, is het noodzakelijk om:

- **Ethische kaders te hanteren:** Principes van rechtvaardigheid zoals weldadigheid, rechtvaardigheid en solidariteit moeten het ontwerp en de implementatie van blockchainsystemen sturen;
- **Innovatie te bevorderen:** Voortdurend onderzoek naar hybride modellen is essentieel om de beperkingen met betrekking tot privacy te overwinnen, terwijl de sterke punten van blockchain behouden blijven;
- **Samenwerking te stimuleren:** Sectoroverschrijdende partnerschappen zijn fundamenteel om technische, juridische en ethische uitdagingen aan te pakken en ervoor te zorgen dat blockchainoplossingen effectief en eerlijk zijn;
- **Transparantie en vertrouwen te verbeteren:** Inspanningen om blockchainsystemen transparanter en begrijpelijker te maken zullen het vertrouwen van belanghebbenden bevorderen en het bredere gebruik ervan stimuleren.

Over het TRUST project

TRUST bevordert een interdisciplinair onderzoeksprogramma, waarbij zowel academische als niet-academische instellingen betrokken zijn, met als doel het begrijpen van de rol van vertrouwen bij de implementatie van digitale technologieën en het voorstellen van concrete ontwikkelingsmogelijkheden.

Uitgaande van de veronderstelling dat de digitale transformatie van de Europese samenleving alleen volledig kan worden gerealiseerd als technologieën zich ontwikkelen binnen een betrouwbare omgeving, analyseert het project de wederzijdse invloed tussen vertrouwen en digitale technologieën om het relationele vertrouwen in interacties tussen mensen, bedrijven en overheden te versterken.

De focus ligt op blockchaintechnologie (BCT) als een van de meest relevante vormen van Distributed Ledger Technology. BCT wordt beschouwd als een technologie die vertrouwen opbouwt, doordat het nieuwe vormen van relationeel vertrouwen creëert. BCT plaatst het vraagstuk van vertrouwen in een nieuwe dimensie die we willen verkennen, in overeenstemming met de initiatieven en kernacties die door de Europese Commissie zijn gepromoot in de mededeling "Shaping Europe's digital future" (COM (2020) 67 final), waarin wordt benadrukt dat vertrouwen en digitale transformatie van de samenleving hand in hand gaan.

Het onderzoeks- en kennisoverdrachtsprogramma richt zich op kernonderwerpen zoals: de ontwikkeling van een passend regelgevend kader voor de effectieve integratie van BCT in een op vertrouwen gebaseerde samenleving; de overgang naar een eerlijke en concurrerende peer-to-peer economie; de toepassingen van BCT op het gebied van AI om veiligheid en vertrouwen te waarborgen; en de ontwikkeling van nieuwe modellen voor collaboratief bestuur in slimme en op vertrouwen gebaseerde steden.

Het consortium bundelt expertise uit verschillende disciplines (juridisch, economisch, technisch), afkomstig uit EU-landen, evenals Israël en China. Complementaire onderzoeksperspectieven, innovatieve opleidingen en internationale/intersectorale samenwerking zullen de loopbaanontwikkeling van medewerkers stimuleren door te onderzoeken hoe het gebruik van digitale technologieën kan bijdragen aan een betrouwbare Europese omgeving, waarin burgers worden versterkt in hun handelen en interacties, en waarin ook economische groei wordt bevorderd.

Partners in het TRUST project



Región de Murcia



Funded by
The European
Union



[Link naar de website van het TRUST project](#)