Jubel.be | Powered by KNOPSPublishing.com

KRITISCHE EVALUATIE VAN DIGITALISERINGSPROJECTEN BINNEN JUSTITIE

Pierre Thiriar

Jubel.be, 6 november 2025.

1. Inleiding

Sinds februari van dit jaar probeer ik mijn democratisch controlerecht uit te oefenen in het kader van de wet openbaarheid van bestuur. Wat een relatief eenvoudige procedure zou moeten zijn, is in de praktijk een uitputtend traject gebleken. Ondanks herhaalde verzoeken en tussenkomsten van de Commissie voor toegang en hergebruik van bestuursdocumenten, bleef een transparante en tijdige verstrekking van de gevraagde documenten uit. Pas op 24 oktober werd mij een deel van de gevraagde stukken toegezonden, maar zelfs dan bleken meerdere documenten gecensureerd of onvolledig. Het is moeilijk dit anders te interpreteren dan als een teken dat er “iets” verborgen wordt en enkel dat feit is al bijzonder verontrustend. In een democratische rechtsstaat hoort openbaarheid de regel te zijn, zeker bij een federale overheidsdienst die net de wet dient te beschermen en toe te passen. Het is dan ook zorgwekkend vast te stellen dat de Belgische FOD Justitie ogenschijnlijk zelf een loopje neemt met de wetten van dit land.

2. GDPR/AVG en gegevensbescherming

De bekomen documenten tonen dat de aanpak van gegevensbescherming voor verbetering vatbaar is. Zo wordt in 2021 opgemerkt dat bij inzage van systemen door het Digital Transformation Office (DTO) pas “in een later stadium eventueel een DPIA opgesteld moet worden” – een aanwijzing dat initiële projecten vaak zonder directe Data Protection Impact Assessment van start gingen. Er lijkt ook geen geïntegreerde tooling te zijn voor AVG-compliance in de beginfase: pas in 2023 wordt gesproken over een **“GDPR tooling”** waarvoor men nog de vereisten opstelt en een bestek moet uitschrijven. Onduidelijkheid over de verwerkingsverantwoordelijkheden blijkt eveneens een issue. Een audit van EY stelde vast dat er onduidelijkheid heerst over wie welke rol heeft en dat dit expliciet in kaart gebracht moest worden. Sterker nog, die audit identificeerde **twintig risico’s (waarvan negen hoog)**, met als een van de hoofdthema’s een **gebrek aan conformiteit met wettelijke processen en procedures** binnen Justitie. Dit wijst op hiaten in de naleving van de AVG-regels. Uit de stukken blijkt dat men in 2021 en 2022 haast moest maken met basisvereisten: alle entiteiten moesten **ASAP een inventaris van verwerkingsactiviteiten** opstellen of bijwerken (met steun van de

dienst Informaticabeveiliging & Gegevensbescherming), eventueel aangevuld met DPIA's, zodat deze na validatie door de DPO in het register opgenomen konden worden. Het feit dat dit als dringende actie werd opgelegd, suggereert dat eerder **nog niet alles op orde was** (bijv. geen volledig register of up-to-date DPIA's).

Samengevat wordt gegevensbescherming wel erkend, maar zijn er duidelijke tekortkomingen: tooling was lange tijd afwezig of zwak, DPIA's werden uitgesteld en de **verwerkingsverantwoordelijkheid** was onvoldoende verankerd of duidelijk, zodat pas via audits en werkgroepen stappen werden gezet om dit te verbeteren.

3. Veiligheid, cybersecurity en data-integriteit

Ook op het gebied van digitale veiligheid signaleren de documenten meerdere pijnpunten. In een actiepuntenlijst begin 2022 wordt bijvoorbeeld een nieuw risico toegevoegd **"m.b.t. cybersecurity"**: men had **te veel kritische beveiligingsproblemen** vastgesteld en vreesde dat men die niet binnen de vooropgestelde timing kon aanpakken. Dit risico is expliciet toegevoegd aan de risicoregister, wat suggereert dat de beveiligingsomgeving destijds als acuut zorgelijk werd beoordeeld.

Concrete maatregelen drongen zich op: zo werd de aankoop van **Microsoft E5-licenties** (met uitgebreidere security-functionaliteiten) goedgekeurd met RRF-geld (Europees Relance Fonds) – een aanwijzing dat de bestaande Microsoft-omgeving niet voldeed aan de gewenste cyberbeveiligingsstandaarden en men extra investeringen nodig had voor betere authenticatie, autorisatie en auditing. Pas in 2024 is er sprake van een formeel cybersecurity-beleid: het directiecomité keurde toen een beleidsraamwerk goed, waarbij eindelijk *"beleid en procedures… voor informatiebeveiliging en cyberveiligheid"* zouden worden gedocumenteerd en opgezet – eerdere vergaderingen vermeldden dat dit agendapunt herhaaldelijk was uitgesteld.

Dit wijst erop dat tot voor kort een geïntegreerd veiligheidsbeleid ontbrak of slechts fragmentarisch bestond. Verder zijn er indicaties van zwakke punten in infrastructuur en

toegangscontrole. Zo ontstond discussie over het beheer van de **Azure-cloudomgeving**: men debatteerde of dit naar een apart “Cloud Center of Excellence” moest gaan. De **operationele controle** over deze cloud werd onderwerp van getouwtrek tussen de centrale ICT-dienst en de “Crossborder”-entiteit. De ICT-directeur JDL uitte bezorgdheid dat door verschuiving van cloudbeheer zijn team de grip zou verliezen en het moeilijk zou worden later de controle te hernemen. Dit illustreert zorgen over **controle over data en infrastructuur**: wie beheert kritieke systemen en kunnen magistratuur of FOD Justitie daar zelfstandig op vertrouwen? Positief is dat men in de latere beslissing koos voor gezamenlijke aansturing en het voornemen om het cloudbeheer “zo spoedig mogelijk” terug volledig bij de ICT-dienst onder te brengen, maar die oplossing benadrukt juist dat eerder de verantwoordelijkheden diffuus waren. Over concrete incidenten (zoals datalekken of hacks) reppen de documenten niet expliciet, maar de **talrijke kritieke punten** en noodzaak tot ingrijpende maatregelen suggereren dat de **data-integriteit en infrastructuurveiligheid** kwetsbaar waren. Zo vermeldt een directieverslag dat Justitie **redelijk conform** de CCB-richtlijnen voor cyberveiligheid is, maar toch worden **two-factor authentication** en strengere policy’s aangesneden als aandachtspunt.

Kortom, op veiligheidsvlak waren er **zwakke plekken en vertragingen in het nemen van maatregelen**, hoewel men recent versneld beleidskaders en investeringen heeft doorgevoerd om deze lacunes te dichten.

4. Databeheer, controle over gegevens en tussenkomst van derden

Uit de stukken blijkt een versnipperde governance rond data en IT-projecten, met onduidelijke eigenaarschap en inmenging van externe spelers (zoals consultants) op cruciale domeinen. Zo vroegen leden van de DTP-stuurgroep al in 2021 om **een globaal overzicht** van alle stuurgroepen en werkgroepen (inclusief samenstelling en planning). Dit verzoek – om na te gaan “wie betrokken is in welk orgaan en te verzekeren dat er geen overlap is” – toont dat de projectstructuur zo gefragmenteerd was dat men het overzicht kwijt was en mogelijk dubbel werk of inconsistent beleid ontstond.

Ook de **governance van toegangsrechten** en data-eigenaarschap bleek onvoldoende uitgewerkt. In een bespreking van een nieuwe toepassing (een *Recidivemonitor*) wordt expliciet gesteld dat *"de governance (wie krijgt toegang tot wat enz.) nog moet worden uitgewerkt"*. Met andere woorden: er was een tool in ontwikkeling, maar de basisvraag wie welke data mag zien of beheren lag nog open. Dit wijst op **slechte datagovernance** en potentieel risico op ongecontroleerde data-inzage.

Daarnaast speelt de rol van externe partijen en consultants. Meerdere keren valt op dat externen een grote vinger in de pap hebben, wat vragen oproept over controle. In de allereerste DTP-stuurgroepvergadering werd al gevraagd **"wie/hoe zal de consultants controleren?"**, gezien de omvang van hun betrokkenheid. Dit impliceert dat consultants op dat moment belangrijke rollen vervulden in het digitaliseringsprogramma, zonder duidelijk kader van verantwoording of toezicht.

Inderdaad blijkt later dat bij de aparte IT-entiteit *"Crossborder"* **meer dan driehonderd externe consultants** actief waren en dat diezelfde consultants zelfs het budget beheerden. Een lid van het directiecomité uitte hierover scherpe kritiek: *"het is een probleem dat consultants het budget van Crossborder beheren"* – **Justitie moet de controle terugkrijgen**, en daarom werd Team Begroting & Beheerscontrole opgedragen alle rekeningen te controleren. Hierbij werden al **onregelmatigheden gedetecteerd**, hetgeen onderstreept dat de invloed van derden had geleid tot mogelijke financiële of organisatorische wantoestanden. Dit is een significant voorbeeld van uit handen geven van de controle: een externe of hybride dienst die met overheidsgeld werkt, maar niet onder directe ambtelijke sturing stond, met alle risico's van dien.

Ook binnen de interne structuren was er onduidelijkheid over rolverdeling en eigenaarschap van systemen. Zo moesten DTO, de centrale ICT-dienst (SD ICT) en de "CBE" (?) afspraken maken over **wie beslist op welk niveau** – men vroeg om uniformiteit in de verschillende stuurgroepen en duidelijke escalatielijnen naar de DTP-stuurgroep. Dat deze vraag expliciet gesteld wordt, toont dat de bestuursstructuur diffuus was. Verder wordt erkend dat er **schaduw-IT** bestaat: een voorstel noteert dat bepaalde *"Shadow IT-applicaties"* buiten scope

vielen, wat betekent dat sommige door gebruikers zelf ontwikkelde of ingevoerde tools niet in het officiële IT-plan waren opgenomen – een recept voor ongecontroleerd databeheer.

Al met al schetsen de documenten een beeld van **versnipperd databeheer en governance**: te veel verschillende initiatieven zonder centrale regie, onduidelijke grenzen tussen wat de FOD Justitie zelf beheert en wat externen of andere entiteiten doen en een noodzaak om de **eigendom en toegang tot data** duidelijker af te bakenen. De recente stappen (zoals het opvragen van overzichten, invoeren van governance-documenten, etc.) geven aan dat men dit probleem inziet en tracht te remediëren, maar in de onderzochte periode was dit een belangrijk knelpunt.

4. Inzage in gerechtelijke dossiers en monitoring van digitale activiteiten van magistraten

De onafhankelijkheid van magistraten dreigde in het gedrang te komen door bepaalde digitale initiatieven, maar hierop zou (in ieder geval op papier) alert gereageerd zijn. Een kernpunt is de **toegang van IT-projectleden tot rechterlijke dossierinformatie**. In de eerste DTP-stuurgroep (juni 2021) werd het mandaat van de DTO-leden besproken: de stuurgroep stelde **uitdrukkelijk** dat zij **niet bevoegd** is om DTO-leden een mandaat te geven “om de inhoud van dossiers te bekijken”. Dit werd bevestigd door de DTO-verantwoordelijken zelf: zij argumenteerden dat voor hun opdracht inzage in inhoudelijke dossierdata *“absoluut niet noodzakelijk”* is, aangezien het hen enkel om technische informatie en procesflows te doen is.

Uiteindelijk heeft de stuurgroep zeer strikte voorwaarden geformuleerd om iedere potentieel ongepaste inzage te voorkomen: **alleen IT-technische informatie** mag worden geraadpleegd, **toegang moet steeds vooraf aangekondigd** zijn, **nooit individuele dossierinhoud** en de nood tot inzage moet op voorhand gemotiveerd worden. Bovendien moeten betrokken DTO-medewerkers minstens een geheimhoudingsverklaring (NDA) tekenen en indien er toch gevoelige gegevens zouden verwerkt worden, zou in een later stadium een DPIA moeten volgen. Deze maatregelen laten zien dat men zich bewust is van het gevaar dat IT-personeel (mogelijk behorend tot de uitvoerende macht of privé-consultants) in systemen van magistraten zou kunnen kijken, wat de rechterlijke onafhankelijkheid kan schaden. Het

expliciet uitsluiten van inzage in de inhoud van gerechtelijke dossiers door DTO-leden is bedoeld om elke indruk van inmenging te vermijden.

Wat **monitoring van digitale activiteiten van magistraten** betreft (bijvoorbeeld het bijhouden van hun computergebruik, e-mail, dossiers die ze raadplegen, enz.), wordt in de documenten niets expliciet vermeld. Er worden geen gevallen of systemen beschreven die systematisch het doen en laten van magistraten digitaal volgen. Dat betekent niet per se dat zulke monitoring niet bestaat, maar in elk geval is er **geen transparante vermelding** ervan in deze verslagen. Dit op zichzelf kan worden gezien als een gebrek aan informatie (zie punt 6), maar het kan ook betekenen dat men formeel (nog) niet aan dergelijke monitoring doet – mogelijk juist omwille van de gevoeligheid.

In elk geval tonen de stukken wel aan dat de magistratuur beschermd wilde worden: men was zeer waakzaam om te voorkomen dat digitale transformatieprojecten de **onafhankelijkheid van de rechterlijke orde** zouden compromitteren. Als voorbeeld hiervan geldt ook dat DTO-leden eerst moesten proberen info via de organisatie te verkrijgen en pas als niemand bereikt werd, **via de stuurgroep toestemming konden vragen – een pragmatische stap om te zorgen dat magistraten niet zonder hun weten "gescreend" worden door externen**.

Samengevat is er een duidelijk bewustzijn van de delicate balans tussen digitalisering en rechterlijke onafhankelijkheid. Risico's zoals te brede toegangsrechten of onzichtbare monitoring worden (voor zover de documenten prijsgeven) tegengegaan met strikte protocollen, al blijft de precieze naleving daarvan moeilijk te beoordelen op basis van de beperkte informatie.

6. Achtergehouden of ontbrekende informatie in verslaggeving

Er zijn meerdere aanwijzingen dat niet alle relevante informatie expliciet in de documenten is opgenomen, wat vragen oproept over transparantie. Ten eerste valt op dat de verslagen regelmatig melding maken van zaken **zonder inhoudelijke toelichting**. Zo wordt in het directiecomité-verslag van oktober 2021 verwezen naar een dossier *"GBA – SIDIS"*, waarbij de

voorzitter een ontwerpantwoord aan de Gegevensbeschermingsautoriteit toelicht en de deadline voor verzending vermeldt. Hoewel duidelijk is dat er een belangrijk privacy-issue speelt (de GBA is erbij betrokken), wordt in het verslag zelf **niet beschreven wat het probleem precies inhoudt** noch wat de kern van het antwoord is – de lezer weet enkel dat er geantwoord zal worden. Cruciale informatie over de aard van de SIDIS-problematiek blijft zo buiten beeld. Dergelijke hiaten komen vaker voor: beslissingen worden genotuleerd ("het antwoord zal overgemaakt worden… en gevalideerd"), maar de onderliggende context of discussie wordt niet gedeeld.

Daarnaast is er sprake van bewuste weglating van detail in de notulen. In de DTP-stuurgroepverslagen staat expliciet dat *"enkel de punten waarvoor een beslissing nodig was of waarover opmerkingen geformuleerd waren"* zijn opgenomen, en dat **voor de overige agendapunten verwezen wordt naar de PowerPointpresentatie**. Dit betekent dat allerlei informatie en toelichting die tijdens de vergadering werd gegeven (vb. statusupdates, demo's, inhoudelijke stand van zaken) niet in het schriftelijk verslag verschijnt. Belanghebbenden die niet aanwezig waren of achteraf het document lezen, krijgen dus enkel de conclusies mee, niet de volledige informatie. Men zou kunnen stellen dat dit de verslagen beknopt houdt, maar het **achterhouden van de discussie-inhoud** kan ook strategisch gebeuren om minder positieve details of twijfels niet op papier te hebben.

Opvallend zijn ook de vele **"XXXX" aanduidingen** in de teksten, wat duidt op weggelakte of weggelaten informatie. Namen van personen of gevoelige onderdelen zijn consequent onleesbaar gemaakt. Bijvoorbeeld: *"Feedback XXXX: Momenteel is het GeBeCom de enige wettelijke beslissingsstructuur…"*, waar klaarblijkelijk de naam van de feedbackgever is verwijderd. **Evenzo staan in het directiecomité-verslag van 2023 hele passages met "XXXX", onder meer rond de ontdekking van onregelmatigheden bij Crossborder.** Hierdoor is het niet duidelijk **wie** iets gezegd heeft of **welk onderdeel** concreet bedoeld wordt. Dit kan gedaan zijn om persoonlijke gegevens te beschermen of confidentiële elementen te verhullen, maar het resultaat is een document dat op bepaalde punten weinig prijsgeeft.

Tevens zijn er indicaties dat informatie bewust is **achtergehouden of vertraagd verspreid**. Zo wordt er ergens vermeld dat *"er is nog geen communicatie van dit project gedaan naar het college, dit moet opgepikt worden"* – met andere woorden, men had nagelaten een belangrijk project tijdig met een belangrijke partner te delen. Ook dat is een vorm van informatie niet (tijdig) delen. Ten slotte moet opgemerkt worden dat de documenten zelf second-hand informatie zijn (verslagen en nota's). Mogelijk werden nog gevoeligere zaken mondeling besproken of in vertrouwelijke bijlagen gezet waar ik geen zicht op heb. De aanwezigheid van vragen in de opdracht over "expliciet weggelaten uit verslagen" suggereert dat er vermoedens zijn dat bepaalde pijnlijke punten niet zwart-op-wit gezet zijn.

Deze analyse bevestigt in elk geval dat de verslagen *niet alles vertellen*: er is een zekere **gebrekkige transparantie**, zowel door bewuste redactie (weglatingen) als door een zeer beperkte verslagstijl die veel onderwerpen onbesproken laat.

7. Financiële malversaties, wanbeheer en inefficiënties

De digitaliseringsprojecten gaan gepaard met aanzienlijke budgetten, maar de realisatie daarvan lijkt gekenmerkt door vertragingen, onderbenutting en mogelijke onregelmatigheden. Uit een monitoringrapport blijkt dat van de **124 miljoen euro** aan investeringskredieten (IDP) voor ICT-projecten in 2021 slechts **58,4%** vastgelegd was (gecommitteerd) en amper **14,6%** effectief uitgegeven. Dit halverwege het begrotingsjaar – met een dreigende stopzetting van bestellingen begin december – wijst op ernstig **achterophinken op planning en besteding**. Sommige projecten liepen vertraging op omdat er geen beschikbare raamcontracten meer waren, een teken van planningsfouten of gebrekkige aanbestedingsstrategie waardoor men budget niet tijdig kan inzetten. Dergelijke inefficiënties leiden tot het risico dat middelen ongebruikt terugvloeien of dat deadlines niet worden gehaald.

Die vrees wordt elders expliciet bevestigd: voor het project **JustPrison** bijvoorbeeld meldt ICT-directeur JDL dat het *"vertraging oploopt met risico dat de deadline van eind 2023 niet gehaald wordt"*, en dat men de contractuele en budgettaire gevolgen van die vertraging moet

inschatten. Later blijkt JustPrison zelfs **twee jaar achter op schema** en van *"gebrekkige kwaliteit"*, waarop het directiecomité besluit een gespecialiseerd advocatenkantoor inzake overheidsopdrachten in te schakelen. Dit duidt op mogelijk wanbeheer of een falende leverancier: men moet juridische stappen overwegen om het project vlot te trekken of aansprakelijkheden te beoordelen.

Een dergelijk ingrijpen (extern juridisch advies) wijst doorgaans op ernstige problemen, zoals contractbreuk, wanprestatie of mismanagement. Ook andere projecten kenden **"delay notes"** en herplanningen – er wordt gesproken over opstellen van nota's om vertragingen bij JustJudgment te verantwoorden en over gefaseerde planningen die telkens bijgesteld worden. De ambitie was hoog (veel simultane IT-hervormingen), maar de realisatie hapert: releases nemen meer tijd door bijkomende vereisten en formaliteiten, en het goedkeuringsproces *"vertraagt de planning"*.

Naast inefficiëntie is er ook sprake van mogelijke **financiële malversaties of wanbeheer**. Zoals eerder vermeld, ontdekte men bij de dienst Crossborder dat externe consultants de budgetten beheerden en dat er **onregelmatigheden** aan het licht kwamen. Het directiecomité liet daarop alle rekeningen doorlichten en besloot Crossborder onder strakker hiërarchisch gezag te plaatsen. Hoewel de precieze aard van de "onregelmatigheden" niet in het verslag staat (mogelijk fraude, foutieve uitgaven, of overschrijding van bevoegdheden), is het duidelijk dat er financiële controleproblemen waren – potentieel dus **malversaties** in de breedste zin (zij het misbruik, onrechtmatige besteding of gewoon chaotisch beheer).

Het feit dat Justitie "de controle moet hernemen" over budgetten en dat zelfs een screening van de hele dienst wordt gepland, wijst op **ernstige bezorgdheid over financieel beheer**.

Verder zijn er tekenen van **wanbeheer** in het zin van slechte coördinatie en verspilling. Zo had Crossborder opdrachten naar zich toegetrokken "die normaliter door de dienst Procurement en Team ICT werden uitgevoerd", wat mogelijk tot dubbel werk of inefficiëntie leidde. Dat een aparte entiteit parallel aan bestaande diensten hetzelfde werk ging doen, suggereert gemiste synergiën en potentieel hogere kosten (bv. consultants inhuren waar interne diensten het

hadden kunnen doen). We zien ook dat projecten soms zonder duidelijke scope startten en achteraf bijgestuurd moesten worden: bijv. het **smartphoneproject** voor justitiepersoneel werd *"complex"* genoemd, met onduidelijke governance en scope, waardoor tijdens de bespreking pas besloten werd dat deze "duidelijk moeten worden gemaakt". Dit soort ad-hoc bijsturen verraadt een initiële onderschatting of misplanning. Daarnaast zijn deadlines geregeld niet gehaald of ad interim aangepast (bijv. de gefaseerde activatie van e-PV's per regio, ondanks een eerdere afspraak om gelijktijdig live te gaan), wat de streefdoelen steeds opschuift en op de werkvloer tot verwarring leidt.

Kortom, de financiële en planningscomponent van de digitalisering bij Justitie toont een **behoorlijk chaotisch beeld**: onderbenutte budgetten, overschreden termijnen, projecten die jaren uitlopen en zelfs juridische stappen vereisen, plus een governance die externe uitvoerders te veel vrijheid gaf met overheidsgeld.

Dit alles wijst op **inefficiënties en mogelijk wanbeheer** die de digitale ambities fnuiken. De vraag of er zelfs sprake is geweest van bewuste malversatie (fraude) blijft open, maar het feit dat "onregelmatigheden" zijn vastgesteld suggereert dat dit niet wordt uitgesloten en op zijn minst onderzocht wordt.

8. Risicoanalyses

Risicoanalyses zijn zeker aanwezig binnen de digitaliseringsprojecten, maar de diepgang en opvolging ervan variëren. In de vergaderdocumenten van de DTP-stuurgroep is standaard een agendapunt **"Risico's & issues"** voorzien. Daarin worden geïdentificeerde risico's doorgaans overlopen en soms bijgestuurd. Een voorbeeld: in een vroeg verslag (Stuurgroep van 30-06-2021) staat dat de risico's "zijn overlopen" en dat er **geen verdere vragen** bij gesteld werden – wat suggereert dat men een lijst had, maar dat er op dat moment geen diepe discussie nodig of gaande was. In latere bijeenkomsten zien we echter dat risicoanalyse serieuzer wordt aangepakt, zeker wanneer externe partijen zoals EY worden ingeschakeld. Zo rapporteert een AVG-conformiteitsaudit (uitgevoerd door EY) dat men **twintig risico's (negen hoog)** heeft geïdentificeerd voor het digitale JustJudgment-project, gegroepeerd in thema's. Belangrijk is

dat daar de **meest kritieke risico's expliciet benoemd** worden: onder andere het *gebrek aan conformiteit met wettelijke processen* (wat de complexiteit verhoogt) en de vele stakeholders met uiteenlopende verwachtingen. Dit duidt op een grondige risico-evaluatie die breder kijkt dan louter technische aspecten – ook juridisch-procedurele en organisatorische risico's komen zo boven water. Het rapport benadrukt dat er "nog werk aan de winkel is" om alle risico's te mitigeren, hoewel sommige al zijn afgenomen door intussen gestarte initiatieven.

Naast specifieke audits werd ook intern werk gemaakt van risicobeheer. Eind 2020 was het directiecomité zich bewust dat er structureel iets moest gebeuren: men noteerde dat het noodzakelijk is over de nodige middelen te beschikken, zowel centraal (vervanging van de risk officer) als binnen de entiteiten (rechtscolleges), om aanvullende beveiligingsmaatregelen te nemen. Dit impliceert dat er een risicoverantwoordelijke was (of moest zijn) en dat men risicomanagement wilde verankeren doorheen de hele organisatie.

Toch laat de praktijk zien dat risicoanalyses soms pas achteraf of reactief gebeurden. Het toevoegen van het cybersecurity-risico in 2022 (zie punt 3) toont dat men een belangrijk risico herkende *nadat* kritieke punten al waren vastgesteld, en dit dan als nieuwe bevinding in de register opnam. Ook werd gemeld dat de optelsom van risico's in een bepaalde werkstroom maakte dat die als geheel op "rood" werd gezet – men gaf dus dashboards of kleurcodes aan om aan te duiden dat een project/werkstroom in gevaar was.

Qua **grondigheid** lijken sommige risicoanalyses vrij gedetailleerd en actiegericht. De eerder genoemde EY-audit komt bijvoorbeeld met aanbevelingen: men spreekt over het opstellen van een RACI-matrix (rollen en verantwoordelijkheden duidelijk toewijzen) en het belang van samenwerking en gestandaardiseerde documentatie om privacyrisico's aan te pakken. Ook moest eerst het proceshuis rond privacy op orde zijn vooraleer een AVG-tool effectief zou renderen – een belangrijk inzicht uit de risicoanalyse.

Belangrijke **toprisico's** die ik uit de documenten afleid, zijn: **cybersecurity-incidenten** (zie punt 2), **niet-naleving van wetgeving** (AVG, procedures – zie punt 8), **vertragingen die tot budgetverlies leiden** (RRF-deadlines bijvoorbeeld, waarbij vertraging een risico is dat

subsidies mislopen) en **mensen/kennis risico's** (zoals onvoldoende opgeleid personeel voor privacy compliance, aangegeven door magistraten). De **hoofdrisico's** komen dus overeen met de tien thema's zelf: privacy, security, governance, onafhankelijkheid, enz., worden ook intern als risico gezien. Bijvoorbeeld, in de risicolijst van EY wordt genoemd dat er een *"gebrek aan conformiteit met wettelijke processen"* is – dit is zowel een juridisch risico (voor punt 8) als een operationeel risico omdat het de complexiteit verhoogt.

Wat de **adequaatheid** betreft: men *heeft* risicoanalyses, maar de effectiviteit hangt af van opvolging. Sommige risico's lijken lang aan te slepen. Een notule wijst erop dat de trage uitvoering van de in 2018 gekozen strategie ertoe leidt dat resultaten nog niet zichtbaar zijn, ondanks dat risico's en maatregelen al in 2018 geïdentificeerd waren. Dit suggereert dat hoewel risico's in kaart gebracht zijn, de **mitigatie traag** verloopt. Toch zien we ook snelle reacties, bv. het inhuren van een advocatenkantoor voor JustPrison als mitigerende maatregel voor contractrisico's, of het uitbreiden van licenties om securityrisico's te verlagen.

Over het algemeen zijn de belangrijkste risico's bekend en beschreven in de stukken, maar de documenten tonen ook dat Justitie **worstelt om de risico's tijdig en afdoende te beheersen** (soms door gebrek aan mensen of middelen, soms door complexiteit).

9. Naleving van wetgeving (aanbestedingen, GDPR, etc.) en mogelijke strafbare feiten

De naleving van diverse wettelijke kaders vormt een rode draad door de documenten, vaak in de vorm van problemen of aandachtspunten. Op het gebied van **aanbestedingswetgeving** zijn er duidelijke indicaties van moeilijkheden. Het meest sprekende voorbeeld is opnieuw het JustPrison-project: door de *"gebrekkige kwaliteit van de geleverde diensten"* en de enorme vertraging besloot men een advocatenkantoor gespecialiseerd in overheidsopdrachten in de arm te nemen. Dit impliceert dat men juridisch advies nodig had mogelijk om een contract te herzien, claims in te dienen of een leverancier in gebreke te stellen.

Het kan ook betekenen dat er bij de gunning of uitvoering mogelijk iets misliep dat juridische consequenties heeft. In elk geval toont het dat de FOD Justitie moeite had om via de normale

aanbestedingsprocedure tot een succesvol resultaat te komen en nu **juridische stappen** overweegt, wat vrij uitzonderlijk is en kan wijzen op ernstige contractuele problemen.

Daarnaast was er het issue van de **verlopen raamcontracten** waardoor projecten vertraagden – dit suggereert mogelijk een gebrek aan tijdige aanbesteding of verlenging. Als raamovereenkomsten aflopen zonder opvolger, zit men wettelijk vast (men kan niet bestellen), wat op zichzelf een teken is van **non-compliance met planning/aanbestedingsregels** (immers had men proactief nieuwe moeten afsluiten). Men moest hierop improviseren binnen de wettelijke mogelijkheden, wat kennelijk niet vlekkeloos verliep.

Wat **AVG/GDPR** betreft, is er aantoonbaar strijdigheid geweest met de verplichtingen, althans tot voor kort. Zoals onder punt 1 besproken, had de FOD Justitie kennelijk niet alle verplichte registers en DPIA's op orde in 2021, gezien de inhaalbeweging die toen ingezet is. Dit is strikt genomen een **niet-naleving van de AVG** (elke overheid moet een register van verwerkingsactiviteiten hebben en risicoverwerkingen in kaart brengen). De tussenkomst van de Gegevensbeschermingsautoriteit (GBA) in het SIDIS-dossier bevestigt dat er een privacy-issue was waarop de toezichthouder heeft moeten optreden. Hoewel details ontbreken (zie punt 6), is het feit dat de GBA een antwoord eist, een signaal dat de FOD Justitie mogelijk in overtreding was of op zijn minst vragen moest beantwoorden over gegevensbescherming.

In de EY-audit wordt gebrek aan conformiteit met wettelijke procedures expliciet als hoog risico genoemd. Verder blijkt uit de geciteerde opmerkingen van magistraten dat de FOD Justitie zelf bepaalde **AVG-initiatieven van de rechterlijke orde blokkeerde** (zoals het gebruik van eigen templates) in afwachting van een centraal systeem, wat de vraag oproept of de FOD Justitie de verantwoordelijkheid wel correct neemt of zo mogelijk de rechterlijke orde verhindert om zelf compliant te zijn. Dit spanningsveld kan ook juridische implicaties hebben, want als de rechterlijke macht daardoor niet voldoet aan AVG, waar ligt dan de aansprakelijkheid?

Zijn er aanwijzingen van **strafbare feiten** in de projectwerking? De documenten noemen geen expliciete zaken als fraudeonderzoeken of strafrechtelijke vervolging, maar de term *"onregelmatigheden"* die ontdekt zijn bij Crossborder kan potentieel ook fraude of verduistering omvatten. Omdat consultants het budget beheerden en ambtenaren pas achteraf controleren, is het niet ondenkbaar dat hier mogelijk onrechtmatige uitgaven of zelfverrijking plaatsvond (hoewel ik dat niet kunnen bevestigen uit deze bronnen). Het directiecomité heeft in elk geval ingegrepen *voordat* dit escaleerde: de controle werd teruggehaald naar ambtenaren en Crossborder werd onder het gezag van de voorzitter geplaatst voor een volledige screening. Dit wijst erop dat men iets niet pluis vond – wat zou kunnen variëren van administratief wanbeheer tot potentieel strafbare misdrijven als corruptie of belangenvermenging. In de context van aanbestedingen is ook relevant dat Crossborder blijkbaar taken uitvoerde die tot het domein van de dienst Procurement hoorden. Als daarbij voorschriften omzeild zijn (bijv. directe gunningen zonder procedure onder het mom van Crossborder), dan zou dat in strijd met de wet op overheidsopdrachten kunnen zijn. Concrete aanwijzingen daarvoor staan niet zwart op wit in de verslagen, maar de constructie op zich (een hybride dienst die buiten de gewone structuren opereert) wekt minst genomen de *schijn* dat men reguliere procedures probeerde te omzeilen – iets wat als het bewust is, illegaal kan zijn.

In bredere zin signaleert het gebrek aan compliance dat de FOD Justitie soms de eigen wettelijke regels onvoldoende naleeft. De Inspecteur van Financiën (IF) heeft in minstens één geval kritische adviezen moeten geven (o.a. bij het telefoniedossier, waar uitstel en second opinions nodig waren). Ook zien we dat voor bepaalde constructies (zoals de "hybride dienst" Crossborder) vragen rijzen of die wel reglementair kunnen worden omgevormd naar een traditionele structuur, mede omdat de FOD Justitie nog niet de nodige profielen of expertise in huis heeft die bij Crossborder zitten. Dit geeft aan dat men soms buiten het boekje moest werken om dingen gedaan te krijgen (bijv. projectmatig consultants inschakelen via alternatieve kanalen).

Samengevat: de naleving van regelgeving was niet altijd gegarandeerd. **Aanbestedingsprocedures** verliepen stroef of faalden (waardoor deadlines slipten en

juridische hulp nodig was). **Privacyregels** vergden een inhaaloperatie onder toeziend oog van de GBA. En intern moesten **onregelmatigheden** worden rechtgezet om mogelijke malversaties te stoppen. De documenten onthullen geen expliciete strafbare feiten, maar tussen de lijnen door zijn er voldoende rode vlaggen dat sommige praktijken op het randje (of erover) van de wet waren, wat de FOD Justitie noopte in te grijpen **voordat het escaleerde**.

10. Onafhankelijkheid van de rechterlijke orde en scheiding der machten

De digitaliseringsprojecten leggen een spanningsveld bloot tussen de uitvoerende macht (FOD Justitie) en de rechterlijke macht, waarbij bepaalde digitale systemen en structuren de **scheiding der machten** op de proef stellen. Een prominent voorbeeld is de eerdergenoemde **Crossborder**-dienst. Deze dienst ontstond onder impuls van minister Koen Geens (uitvoerende macht) om boetes te innen, maar opereerde met een bijzondere status (SAT-statuut voor de leidinggevende VF) en verwierf gaandeweg taken en middelen (zoals 300 consultants) die nauw aansloten bij rechterlijke activiteiten. Hierdoor ontstond een hybride situatie: is Crossborder nu onderdeel van de FOD Justitie (uitvoerende macht) of een steunpunt van de rechterlijke orde? De directiecomité-vergadering van mei 2023 besluit Crossborder voorlopig onder het gezag van de voorzitter van het directiecomité (JPJ, hoogste ambtenaar van FOD Justitie) te plaatsen en de hele dienst te screenen. Ook zal nadien beslist worden of Crossborder een aparte dienst blijft of overgeheveld wordt naar Team ICT (binnen de FOD).

Dit wijst op een **centralisatiedrift** vanuit de uitvoerende macht – men trekt een entiteit die op armlengte stond weer dicht naar zich toe. Vanuit het oogpunt van rechterlijke onafhankelijkheid kan dit problematisch zijn: systemen die bijvoorbeeld ten dienste stonden van de rechtbanken of het Openbaar Ministerie vallen zo direct onder de hiërarchie van de FOD Justitie. Dat blijkt ook uit de discussie dat VF (de Crossborder-leidinggevende) *"geen hiërarchische meerdere kan zijn gelet op zijn SAT-statuut"*. Met andere woorden, een externe persoon kan niet zomaar opgenomen worden in de hiërarchie van de FOD. De oplossing om Crossborder onder ambtelijk bestuur te brengen, onderstreept dus impliciet dat de eerdere

situatie governancevragen opriep en dat men nu dreigt over te hellen naar volledige integratie (executieve controle).

Een ander gebied waar onafhankelijkheid speelt, is het beheer van kritieke **IT-infrastructuur** zoals de cloud en authentificatiesystemen. Uit de DTP-stuurgroepverslagen blijkt een discussie over het "Cloud Center of Excellence" en de verdeling van cloudbeheer tussen SD ICT (FOD Justitie) en de entiteit Crossborder (die opdrachten uitvoert die tot de rechterlijke macht behoren). Initiële voorstellen om de Azure-cloud in twee te splitsen – één onder Crossborder, één onder Team ICT – werden uiteindelijk afgewezen ten gunste van één gezamenlijk beheer, aangestuurd door zowel de ICT-directeur als de vertegenwoordiger van Crossborder. Toch is de eindbeslissing dat *"het beheer van de Azure Cloud zo spoedig mogelijk volledig wordt overgedragen aan de Stafdienst ICT"*. Dit betekent dat de uitvoerende macht de volledige controle over de cloudinfrastructuur nastreeft. Aangezien hierop ook toepassingen draaien voor rechtbanken en parketten (bv. JustSign, het digitaal handtekenen van vonnissen, en JustJudgment, het digitale dossier voor rechters), kan men stellen dat de **IT-levensader van de rechterlijke orde onder uitsluitend beheer van de uitvoerende macht komt**.

Mocht de FOD Justitie dat beheer misbruiken (bijvoorbeeld door toegang tot rechterlijke data te nemen of uit te vallen op cruciale momenten), dan raakt dat aan de onafhankelijkheid. De documenten geven geen bewijs van dergelijk misbruik, maar de governance-keuzes centraliseren de macht.

Gelukkig is er ook besef van dit risico en worden waarborgen besproken. Zo vermeldt een nota dat *"in een overgangsfase naar de verzelfstandiging van de Rechterlijke Orde"* de veiligheidsadviseur van Justitie eveneens de voorzitters van de colleges van hoven en rechtbanken zal adviseren, zodat het veiligheidsbeleid **compatibel is met de toekomstige constellatie binnen de Rechterlijke Orde**. Hieruit blijkt dat men rekening houdt met een toekomst waarin de rechterlijke orde meer autonomie krijgt (bijv. eigen IT-structuur of governance los van de FOD). Het huidige digitale transformatieprogramma lijkt dus te opereren in de wetenschap dat de scheiding der machten op termijn sterker benadrukt zal worden. Dat men dit expliciet aanhaalt (veiligheidsbeleid moet passen bij toekomstige

autonome rechterlijke macht) is een positief signaal dat de FOD Justitie de onafhankelijkheid niet uit het oog wil verliezen. **Echter, in de tussentijd – voor die verzelfstandiging realiteit is – hangen de digitale voorzieningen van de rechterlijke macht grotendeels af van FOD Justitie en zijn consultants.**

We zagen reeds onder punt 5 hoe men heeft voorkomen dat DTO-medewerkers dossierinhoud kunnen bekijken. Die afspraak beschermt de **materiële onafhankelijkheid** (inhoud rechterlijke dossiers blijft geheim voor uitvoerende macht). Ook is afgesproken dat *consultatie van systemen steeds vooraf aangekondigd en gemotiveerd* moet zijn, wat transparantie biedt en willekeurige speurtochten voorkomt. Deze afspraken zijn essentieel omdat zonder hen een DTO-lid (ingehuurd door de FOD) misschien in alle ICT-systemen van de rechtbanken kon rondneuzen, wat een flagrante schending van de scheiding der machten zou zijn. Door NDA's te eisen en te beperken tot technische gegevens, heeft men de **institutionele onafhankelijkheid** proberen te vrijwaren.

Toch blijft een zekere frictie voelbaar. De rechterlijke orde heeft eigen noden en initiatieven (b.v. de werkgroep GDPR compliance van parket en zetel, die eigen templates wilde invoeren), maar botst soms op de prioriteiten of bemoeienis van de FOD Justitie. Dit kan gezien worden als inmenging van de uitvoerende macht in zaken die eigenlijk de rechterlijke organisatie aangaan. Gecombineerd met de centralisatie van IT-platformen kan dit de perceptie wekken dat de uitvoerende macht via IT de touwtjes in handen houdt bij Justitie.

Hoewel dat praktisch misschien efficiënt lijkt, is het constitutioneel gezien iets om op te letten. Kortom, **digitale systemen kunnen de onafhankelijkheid ondermijnen als de governance volledig bij de uitvoerende macht ligt**. De documenten tonen zowel het risico daarvan als de pogingen om er paal en perk aan te stellen.

11. Communicatie en Informatie naar magistraten en publiek

Op communicatief vlak schieten de digitaliseringsprojecten tekort in proactieve en inclusieve informatieverstrekking, zowel richting de magistraten zelf als naar het bredere publiek. Intern

zijn er herhaaldelijk signalen dat informatie *niet tijdig of onvoldoende* gedeeld wordt met magistraten en hun vertegenwoordigers. Zo staat er in een actielijst expliciet genoteerd dat er *"nog geen communicatie van dit project gedaan [is] naar het College"* (bedoeld wordt het College van hoven en rechtbanken of van procureurs-generaal) en dat dit alsnog moet gebeuren. Met andere woorden: een project was al in uitvoering of besluitvorming, terwijl magistraten zelf er nog niet over geïnformeerd waren. Dit duidt op **gebrekkige betrokkenheid** van de magistratuur bij de digitale hervormingen – **men wordt voor voldongen feiten gesteld in plaats van meegenomen in het proces**. Pas achteraf constateert men dan dat er communicatie had moeten zijn.

Daarnaast komt uit de stukken naar voren dat communicatie vaak laat op gang komt en vooral via interne kanalen verloopt. Op de vraag *"wanneer kan gestart worden met communicatie?"* antwoordde de beleidscel dat *"algemene communicatie gepland is in de loop van februari"* (blijkbaar vlak voor of rond een lancering). Dit impliceert dat men dikwijls **wacht tot kort voor de oplevering** om magistraten en personeel in te lichten over nieuwe systemen of veranderingen. Een risico hiervan is dat betrokkenen onvoldoende tijd hebben om zich voor te bereiden of dat er onrealistische verwachtingen ontstaan. Men is zich van dat laatste bewust: er wordt benadrukt dat speciale aandacht moet gaan naar **communicatie over wat er op een bepaalde datum wel/niet klaar zal zijn**, zodat de verwachtingen realistisch blijven en de perceptie positief. Het feit dat dit expliciet vermeld wordt, geeft echter aan dat er weldegelijk een kloof bestaat tussen plan en realiteit die kan leiden tot misverstanden bij de doelgroep. Blijkbaar heeft men ervaring met eerdere teleurstellingen of misinformatie, die men nu wil bijsturen door nuance in de boodschap aan te brengen.

Wat de **vorm van communicatie** betreft, lijkt veel te gebeuren via interne platforms (SharePoint, Teams) en per e-mail. Zo worden presentaties beschikbaar gesteld op SharePoint/Teams, en ziet men dat communicatielijnen vaak binnen de ambtelijke hiërarchie lopen (bv. een directeur meldt dat hij een punt op het College van Voorzitters zal bespreken en nadien het directiecomité zal debriefen). Dit top-down model kan ertoe leiden dat de informatie niet altijd de werkvloer bereikt, of pas via via.

Er zijn ook aanwijzingen dat de communicatie vooral reactief is: een vraag van drie balies (advocatenordes) wordt genoemd, en daarop is er kennelijk een reactie geformuleerd dat naar de balie gecommuniceerd is dat digitaal neerleggen van conclusies *nog niet* de papieren versie vervangt. Dit voorbeeld illustreert dat **externen (advocaten, burgers) vaak pas informatie krijgen nadat er onduidelijkheid of ongerustheid ontstaat**. De communicatie naar de balie over Justitie's digitale dossier kwam er blijkbaar nadat men merkte dat er misverstand kon ontstaan over het al dan niet afschaffen van papieren procedures. Hoewel dit adequaat is rechtgezet in een bericht (en zelfs aan DPA medegedeeld, zo lijkt het uit de context), is het punt dat die **voorkomende communicatie ontbrak** – men had de balie proactief kunnen informeren, in plaats van op vraag achteraf.

Een ander aandachtspunt is de **betrokkenheid van magistraten bij de plannen**. Uit de documenten blijkt dat magistraten wel in werkgroepen of aspectgroepen zitten (bv. een referentiemagistraat voor GDPR, of deelname in stuurgroepen), maar dat hun inbreng niet altijd gehoor vindt. Zo gaf ED in de DTP-stuurgroep een krachtige boodschap mee: de magistratuur *heeft* een structuur uitgetekend voor gegevensbescherming (met process owners en referentiemagistraten), maar *"de mensen die er zijn hebben onvoldoende tijd en opleiding"* en er *"zijn te weinig mensen"*. Ook zei hij dat zowel parket als zetel al lang uniformering van templates voorstelden, maar dat dit *"geblokkeerd werd door de FOD Justitie"* in afwachting van een tool die nog steeds niet operationeel is. Deze woorden, die hij nadrukkelijk *"woordelijk in het verslag"* liet opnemen, tonen een zeker **frustratieniveau bij magistraten**: zij voelen zich onderbemand en onvoldoende ondersteund en zien hun initiatieven stranden op het wachten op bovenaf opgelegde oplossingen.

Dit wijst op een communicatie- en coördinatieprobleem: blijkbaar is er niet tijdig of duidelijk overlegd tussen FOD Justitie en de magistraten over pragmatische tussenoplossingen (zoals werken met templates) terwijl men op de grote tool wacht. De magistratuur werd hier dus niet optimaal betrokken of gehoord in besluitvorming, wat de kloof vergroot.

Wat de **burger/het publiek** betreft, vermelden de documenten nauwelijks iets over communicatie naar de bevolking toe. De digitaliseringsprojecten zijn intern gericht (e-Deposit,

JustScan, etc. voor gebruik binnen justitie en voor professionele partijen). Er is geen aanwijzing van voorlichtingscampagnes of publiekscommunicatie over deze nieuwe diensten, behalve mogelijk via de balie of media als ze eenmaal operationeel zijn. Dit gebrek wordt niet expliciet besproken in de verslagen, maar kan als een leemte gezien worden: burgers die te maken krijgen met bv. digitale procedures worden pas laat of indirect geïnformeerd. Een positieve uitzondering is dat er innovatieprijzen en showcases waren (zoals de **Prijs voor de Federale Innovatie** waarbij projecten als het Belgisch Staatsblad-digitalisering, nationaal register gerechtsdeskundigen, DABS genoemd werden) – dat geeft enige publiciteit aan successen, maar is niet per se gerichte communicatie naar eindgebruikers. Concluderend is de communicatiecomponent van de justitieprojecten een zwak punt. **Naar magistraten toe** gebeurt informatievoorziening laat en fragmentarisch, waardoor rechters en parketten soms in onzekerheid verkeren over wat er op hen afkomt. De betrokkenheid is eerder top-down: men stuurt instructies of mededelingen vlak voor implementatie, in plaats van de doelgroep continu mee te nemen of te luisteren naar hun input (getuige de blokkering van veld-initiatieven).

Naar het publiek is er vrijwel geen directe communicatie zichtbaar in deze documenten, wat betekent dat men leunt op tussenpersonen (advocaten, pers, …) of pas communiceert als er iets misloopt. Deze aanpak leidt ertoe dat zowel magistraten als burgers niet ten volle voorbereid of meegenomen worden in de digitale transformatie – een gemiste kans die kan resulteren in weerstand, misverstanden of een lager draagvlak voor de veranderingen. De documentatie zelf onderkent sommige van deze tekortkomingen (men plant immers verbeterde communicatie-acties en dashboards), maar de algemene indruk is dat **transparantie en dialoog** geen prioritaire plaats hadden in de beginfase van de digitalisering. Er is dus duidelijk ruimte voor verbetering op het vlak van communicatie en informatievoorziening.

12. Besluit

Gelet op de aanhoudende terughoudendheid van het ministerie om volledige openheid te verschaffen en met inachtneming van de verschillende strafrechtelijke onderzoeken die zowel

nationaal als op Europees niveau lopen rond de digitalisering van de Belgische justitie, kan er nauwelijks nog sprake zijn van vertrouwen in de zelfregulerende capaciteit van het departement. Het is dan ook niet meer dan logisch dat er dringend werk wordt gemaakt van een parlementaire onderzoekscommissie. Zo'n commissie kan de FOD Justitie eindelijk dwingen om volledig open kaart te spelen en verantwoording af te leggen over beslissingen en praktijken die de fundamenten van de rechtsstaat raken. Alleen volledige transparantie kan hier het morele en institutionele herstel inluiden dat dringend noodzakelijk is.

Pierre Thiriar

Deze bijdrage vertolkt louter de opinie van de auteur in eigen naam.