Sécurité dans la numérisation de la justice pénale :

la cyberrésilience comme tâche commune de la police, de la justice et de l'informatique

Congrès suisse d'informatique de police (SPIK)

16.03.2026 / Jens Piesbergen et Melchior Dörflinger

WAVESTONE

HIS SCHWEIZ
HIJP SUISSE
AIGP SVIZZERA
Kompetenzzentrum digitale Transformation in der Strafjustiz

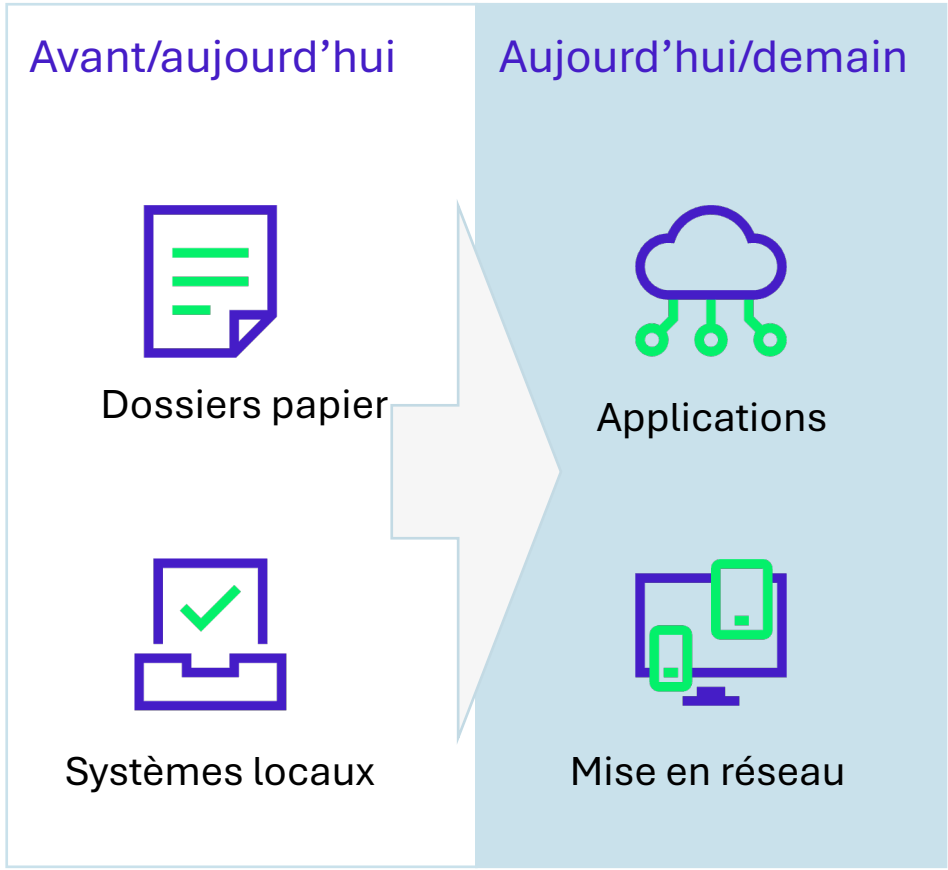
Contexte : transformation numérique de la justice pénale

Les acteurs de la justice pénale vivent une transformation numérique structurelle (efficience, qualité des données, transparence)

- **Les dossiers électroniques** remplacent les dossiers papier
- Gestion des cas et des procédures via des **applications métier** et des applications spécialisées dans l'analyse
- **Échange** de données, documents et preuves **entre les organisations**
- **Interfaces standardisées** ou **plateformes de communication électronique dans le domaine judiciaire** entre la police, les ministères publics, les tribunaux et les organes d'exécution des sanctions pénales, ou les registres.

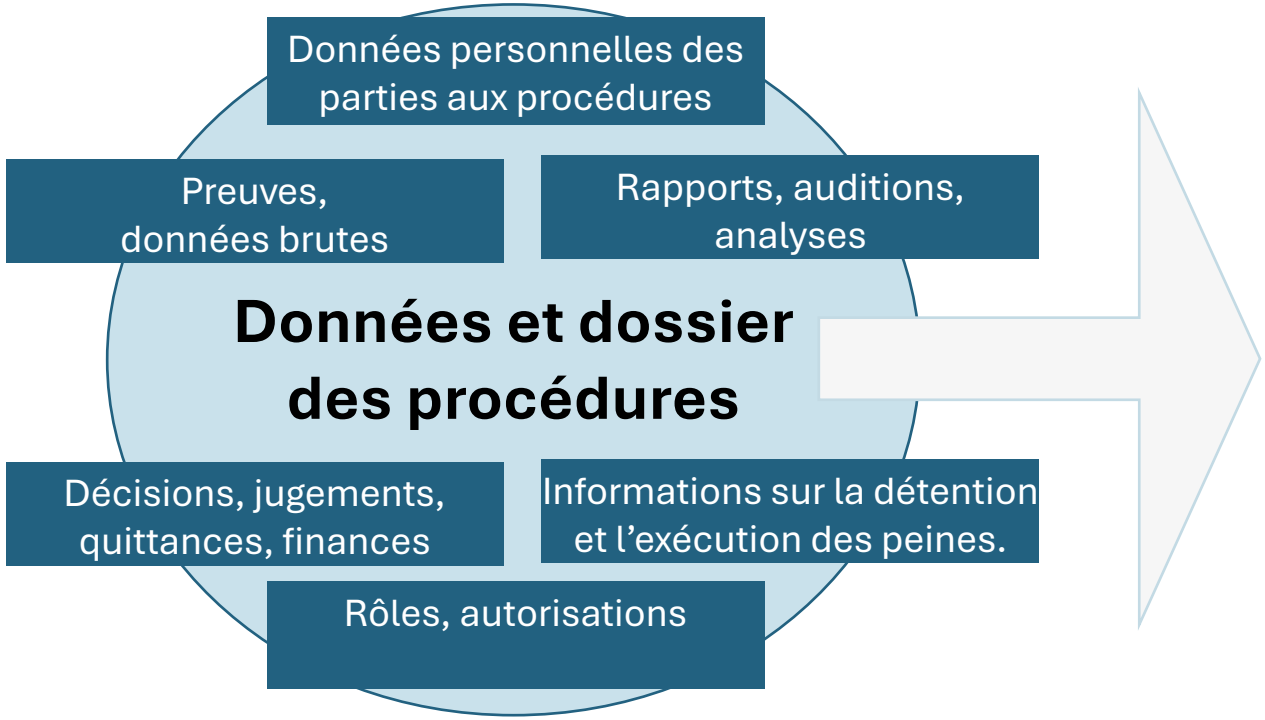
Mise en réseau

- Dépendance élargie et centralisée à des **systèmes (informatiques) stables et dignes de confiance**



Objets à protéger : données sensibles de la justice pénale

Quelles données sont traitées numériquement dans les procédures** ?



- Sensibles
- Liées à la procédure
- Potentiellement utilisables à des fins de manipulation
- Attrayantes pour le chantage et le sabotage

** : procédure préliminaire (investigation/instruction), procédure principale, procédure d'exécution

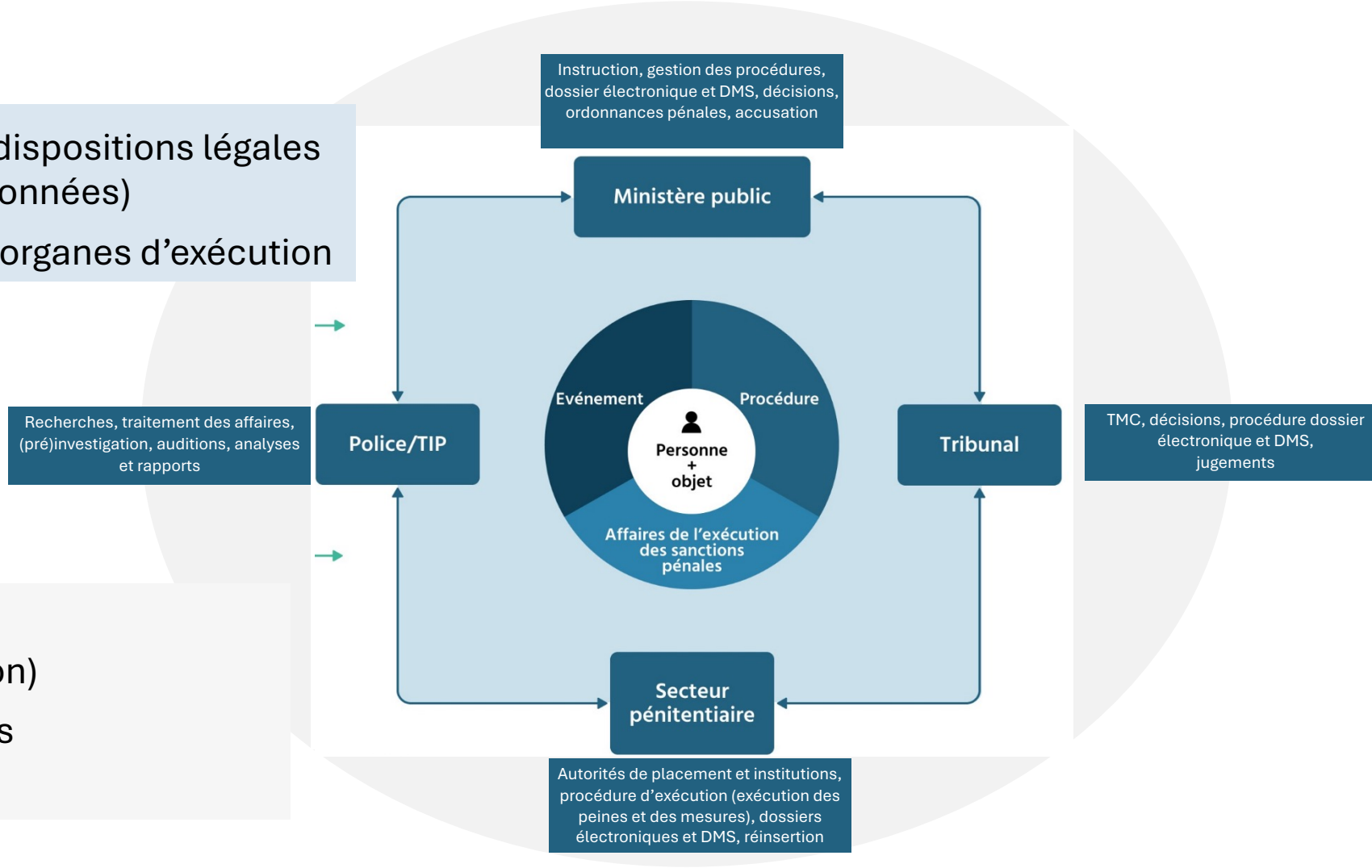
Chaîne pénale : divers niveaux de responsabilité

Responsabilité technique selon les dispositions légales (gestion des procédures, décisions, données)

Police, ministères publics, tribunaux, organes d'exécution

Responsabilité de l'exploitation (exploitation/disponibilité/récupération)

Prestataires de services informatiques (internes/externes aux autorités)



Mise en réseau : nouveaux risques

La mise en réseau assure l'efficience, tout en créant de nouveaux risques systémiques

Différents systèmes

- Diverses applications métier, divers modèles d'exploitation et diverses platesformes : environnement informatique hétérogène

Mise en réseau opérationnelle

- Les flux de données inter-systèmes créent des dépendances et multiplient les points de vulnérabilité

Dépendances communes

- La défaillance d'un système peut paralyser des parties importantes de la chaîne pénale

Différents niveaux de maturité

- Différences cantonales en matière de standards de sécurité et de ressources informatiques
- Prise de conscience au niveau du management

Risques liés à la chaîne d'approvisionnement

- Fournisseurs et prestataires externes en tant que points d'entrée potentiels (chaîne d'approvisionnement)
- Le traitement des données par les autorités elles-mêmes n'est pas cohérent

Protection des données et intégrité

- Données sensibles réparties entre plusieurs systèmes et organisations (applications métier)
- Métadonnées et données de journalisation

État de la menace : principales formes d'attaque

Rançongiciels

Chiffrement des données et menace de publication (double chantage). Possibilité d'interruption de fonctionnement de toute la chaîne pénale.

Hameçonnage et vol d'identifiants

Attaques visant le personnel afin de s'approprier des accès privilégiés. Point d'entrée le plus fréquent.

Attaques DDoS

Surcharge de services critiques. Objectif : perturbation des institutions étatiques, impact politique.

Attaques ciblant la chaîne d'approvisionnement

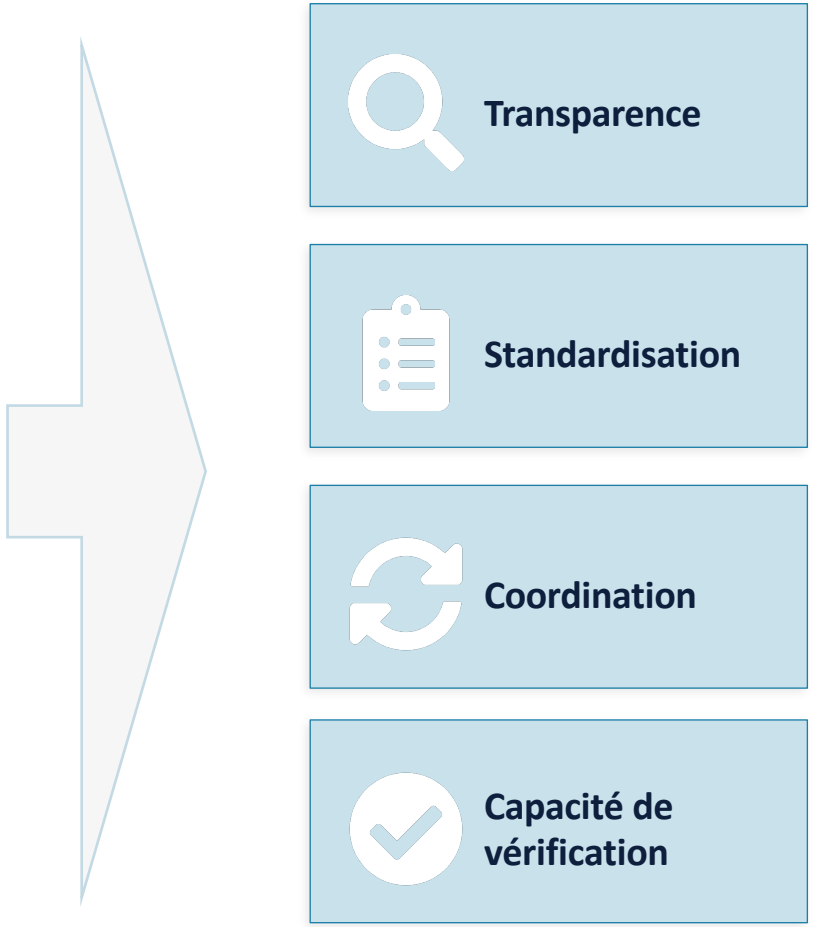
Compromission de fournisseurs ou de composants logiciels (cf. cyberattaque contre l'entreprise Xplain en 2023). Prend l'apparence d'un accès légitime.

Une réalité en Suisse Xplain (2023), attaques de rançongiciels contre des administrations cantonales (2023–2024), vagues de DDoS contre l'administration fédérale (2022–2024)

Modèle de sécurité en association avec différents acteurs

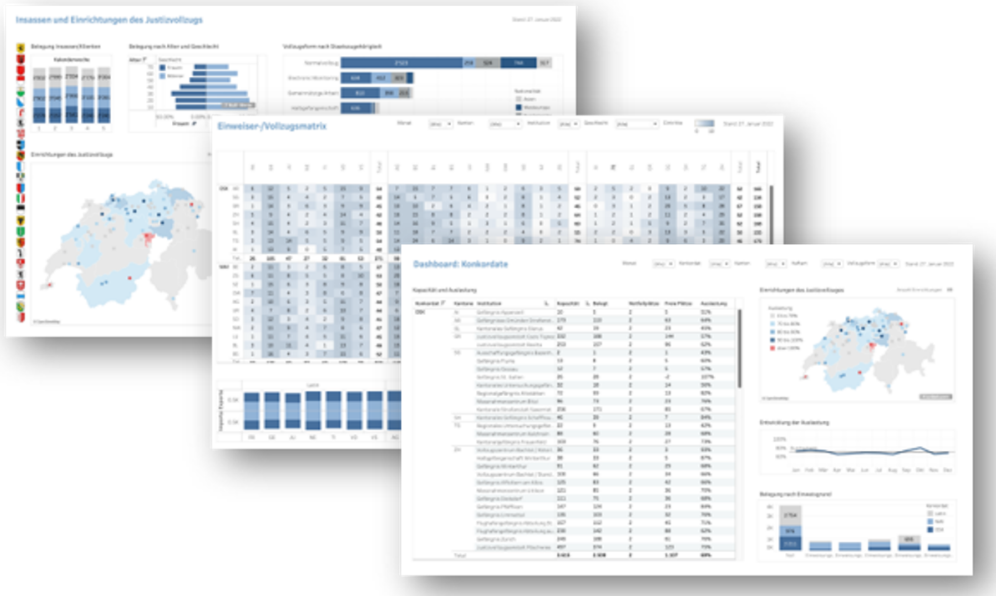
La cybersécurité à trois niveaux

Impact : réduction des risques



Incident de cybersécurité survenu en 2025

SI-ESP : chiffres-clés système d'information dans l'exécution des sanctions pénales



But / Mandat

Fourniture d'informations et de services relatifs aux **données pénitentiaires**

Objectifs / Utilités

- Simplification des processus
  - Livraison de données à des fins statistiques
  - Recherche de personnes détenues
  - Recherche de places disponibles
- Amélioration de la qualité des données grâce à l'automatisation
- Création d'une base légale pour le traitement intercantonal des données personnelles

Prestations

- Statistiques et rapports quotidiens
- Services de recherche

Incident de cybersécurité survenu en 2025 : phase de projet SIESP et canton GR

Livraison de données via des interfaces

- Application métier dans le canton pour le SIESP (@Bedag) et à l'Office fédéral de la statistique
- eCH-0051 v2.11

Données et cas d'utilisation

- Données statistiques : occupation des cellules, recherche de cellules
- Données personnelles sensibles : recherche de personnes détenues
- Données de test productives et anonymisées

Applications et infrastructure informatique

- Infrastructure application métier dans le canton GR avec système de production et de test
- Les défaillances ont un impact opérationnel immédiat sur les résultats du cas d'utilisation

Phase d'intégration et de test

- Intégration sûre de plusieurs applications métier de différents fournisseurs
- Côté cantonal : distinction entre données productives et données de test
- Utilisation des moyens internes disponibles (fournisseurs des applications métier)

Pris en compte dans le projet :

Analyse des besoins de protection

Évaluation systématique du besoin de protection de toutes les informations traitées

Concept SIPD

Concept de sécurité de l'information et de protection des données comme élément obligatoire

Répartition des responsabilités

Règlement clair définissant les responsabilités techniques et opérationnelles pour chaque sous-domaine

Sécurité des fournisseurs

Exigences de sécurité contractuelles et contrôles périodiques

Planification de crise et d'urgence

Planification d'urgence et mesures de reprise, exercices de crise/d'urgence

Instance cantonale de protection des données

Implication précoce de l'instance cantonale de protection des données en tant qu'instance de contrôle

Conclusions

01 Créer de la visibilité

Maîtrisez votre environnement système : qui gère quoi, quelles données circulent et où ?

>> la protection n'est pas possible sans transparence

02 Mener une analyse du besoin de protection

Évaluez systématiquement les données et les systèmes qui nécessitent une protection

>> tirez-en des mesures

03 Définir clairement les responsabilités

Les responsabilités techniques et opérationnelles doivent être clairement définies et faire l'objet d'un contrat

>> il en va de même pour les prestataires externes

04 Planifier les urgences dans un effort commun

Développez des plans d'urgence et mesures de reprise en réseau, car une panne touche tout le monde

>> la réaction doit être coordonnée

05 La sécurité comme tâche permanente

La cyberrésilience est une tâche permanente concernant le domaine technique comme organisationnel

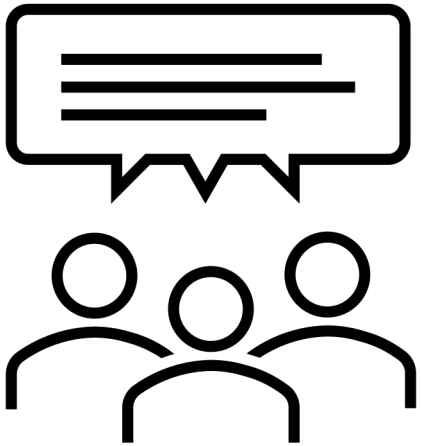
>> ce n'est pas un projet, mais une tâche permanente

06 Mettre en œuvre et adapter les standards

Appuyez-vous sur les standards ISO-27001 ou NIST

>> adaptez-les à votre réalité fédérale

Nous répondons volontiers à vos questions...



Contacts

Jens Piesbergen

Directeur HIJP Suisse

+41 79 473 87 56

jens.piesbergen@his-schweiz.ch

Melchior Dörflinger

Cyber Security Manager Wavestone & CISO HIJP Suisse

+41 76 467 22 41

melchior.doerflinger@his-schweiz.ch

melchior.doerflinger@wavestone.com

Newsletter

www.his-schweiz.ch/fr

HIS Schweiz

Contact Wavestone

www.wavestone.com

WAVESTONE