ARCSI
Association des Réservistes du Chiffre et de la Sécurité de l'Information

Université Paris Cité

Compte-rendu du « Lundi de la cybersécurité »
Lundi 7 Avril 2025

DLP (Data Loss Prevention)
Protection contre la fuite des données sensibles

Organisé par Pr. Ahmed Mehaoua, Béatrice Laurent et Gérard Peliks

Rédigé par Clarisse Veron, étudiante en Master 2 Cybersécurité et E-santé

SOMMAIRE

Introduction

Le **Lundi de la cybersécurité du 7 avril 2025** s'est intéressé à un enjeu central de la protection des systèmes d'information : la **Data Loss Prevention (DLP)**, ou prévention contre la fuite et la perte de données sensibles. Dans un contexte où la donnée est devenue un actif stratégique, souvent qualifié de « patrimoine numérique » des organisations, la capacité à l'identifier, la classifier et la protéger conditionne directement la résilience des entreprises face aux risques internes et externes.

L'intervention principale de la séance a été assurée par **Keren Bismuth**, consultante en cybersécurité au sein de **SOFTEAM Consulting** (groupe Docaposte), spécialiste des projets DLP. Elle a proposé une analyse complète du sujet, en allant bien au-delà de la seule présentation de solutions techniques. Sa démarche s'est attachée à poser des définitions précises (différencier perte, fuite et exfiltration), à explorer les limites de perception dans les communications internes et externes, et à partager une méthodologie pragmatique pour rendre un DLP réellement opérationnel, de la classification des données jusqu'à la gouvernance et l'analyse des incidents.

À mi-parcours de la séance, une séquence spéciale a été consacrée à la présentation de l'**ARCSI** (Association des Réservistes du Chiffre et de la Sécurité de l'Information) par son président, le **général (2S) Didier Looten**. Ancien directeur des systèmes d'information des Armées et aujourd'hui directeur cybersécurité chez Engie, il a présenté les grandes missions de l'ARCSI, son rôle dans la veille et le partage de connaissances en cryptographie et cybersécurité, et a annoncé les **16es Rencontres de l'ARCSI**, qui se tiendront le 22 mai 2025 à Paris sur le thème de la **cryptographie post-quantique**.

I. Comprendre ce que l’on protège : définitions clés

L’un des points forts de l’intervention de **Keren Bismuth** réside dans l’attention portée aux définitions. Avant même d’aborder les solutions techniques, elle a pris le temps de clarifier les termes essentiels du sujet, car selon elle, *« mal nommer les choses, c’est ajouter au malheur du monde »*. Une mauvaise interprétation peut en effet entraîner des incompréhensions, des réponses inadaptées et une couverture de risque insuffisante, notamment dans les échanges avec les assureurs, les clients ou les partenaires externes.

Trois notions sont souvent confondues, alors qu’elles recouvrent des réalités très différentes :

- **La perte de données** désigne une disparition irréversible d’informations. Elle est généralement liée à un incident technique : erreur humaine, problème de sauvegarde, panne de stockage, ou altération des données. Ce type d’événement, bien que souvent accidentel, peut avoir des conséquences opérationnelles majeures pour l’entreprise.

- **La fuite de données** correspond à la divulgation non autorisée d’informations sensibles, tout en conservant potentiellement une copie interne. Elle peut résulter d’un envoi maladroit, d’un usage abusif ou d’un manque de sensibilisation. Elle implique une **exposition** et non une disparition. La fuite peut être intentionnelle ou non, mais elle provient presque toujours d’un **acteur interne**.

- **L’exfiltration de données**, enfin, désigne un vol d’information par un **acteur malveillant externe**, souvent à la suite d’une cyberattaque. L'exfiltration est un acte délibéré, planifié, ciblé, et généralement lié à une compromission technique du système d'information.

Ces distinctions ne sont pas seulement théoriques : elles ont un **impact direct sur la qualification des incidents**, sur la **réaction juridique** à apporter, et sur la **perception** du public et des clients. Comme le souligne Keren Bismuth, un client dont les données ont été exposées peut se montrer plus compréhensif en cas d’attaque externe (exfiltration) que face à une négligence interne (fuite).

Les termes sont souvent mal employés, y compris dans les médias ou les communications officielles. Par exemple, une dépêche évoquant une "fuite de données à la suite d’une cyberattaque" est un contresens : il s’agit d’une exfiltration. De même, l’expression "compromission interne" peut désigner des réalités différentes : elle peut renvoyer à l’usage non autorisé d’un compte resté actif après le départ d’un salarié – un risque particulièrement élevé si ce compte est identifiable sur LinkedIn et toujours accessible via des scans automatisés.

Derrière chaque mot se cachent :

- des **types de menaces** distincts,
- des **acteurs** différents (interne vs externe),
- des **mesures techniques et organisationnelles** spécifiques,
- et des **impacts métiers** hétérogènes.

Mais surtout, ces définitions guident les entreprises dans le **choix de leur stratégie DLP** : un outil efficace contre la perte n’est pas forcément efficace contre la fuite, et inversement. Bien

comprendre ce que l’on cherche à prévenir est donc la première étape incontournable avant toute implémentation.

II. DLP : principes et fonctionnement

Une fois les fondamentaux sémantiques posés, **Keren Bismuth** a abordé le cœur du sujet : le **fonctionnement du DLP** (Data Loss Prevention). Elle l'a défini comme un **ensemble de moyens – techniques et organisationnels – permettant de prévenir la perte ou la fuite de données sensibles**, qu'elles soient en circulation, stockées ou en cours d'utilisation. L'objectif est double : **protéger les données** critiques de l'entreprise tout en **garantissant la conformité réglementaire**, notamment avec des cadres comme le **RGPD**, **HIPAA** (santé) ou **PCI DSS** (paiement).

Elle insiste d'ailleurs sur un point essentiel : un DLP efficace ne se limite pas à bloquer des transferts non autorisés. Il doit aussi être aligné avec la stratégie de l'entreprise, ses usages métiers, son infrastructure, et les types de données à protéger.

Keren Bismuth a ensuite présenté une classification claire des **trois formes principales de DLP**, en fonction de l'**état des données** :

DLP Cloud : données au repos

Ce DLP agit sur les **données stockées** dans les systèmes de fichiers, bases de données, ou solutions cloud (type SharePoint, Google Drive, etc.).

Il permet d'**analyser et contrôler les contenus déjà présents**, pour détecter des informations sensibles mal stockées ou accessibles à trop d'utilisateurs. C'est une protection a posteriori, mais essentielle pour la gouvernance documentaire.

DLP Endpoint : données en cours d'utilisation

Ce DLP se concentre sur ce que l'utilisateur **fait avec la donnée**, sur son poste de travail. Il surveille les actions comme :

- Copier un fichier vers une **clé USB**,
- Envoyer un fichier via **messagerie personnelle**,
- **Imprimer** un document confidentiel.

Il peut bloquer, alerter ou tracer ces actions, selon des règles définies par l'organisation.

DLP Réseau : données en transit

Ce type de DLP inspecte les **flux de données** sur le réseau. Il permet de **détecter et éventuellement bloquer** des envois non sécurisés de données sensibles (emails, transferts FTP, messageries instantanées, etc.).

Il est particulièrement utile pour éviter les **fuites sortantes**, mais peut aussi alerter sur des échanges suspects entre entités internes.

Keren Bismuth rappelle les **limites structurelles du DLP** : l'outil ne traite que les données numériques **au sein du système d'information**. Or, les fuites peuvent également survenir :

- Lors d’une **réunion projetée à l’écran**,
- Au cours d’un **appel téléphonique**,
- Ou même via une **photo d’un document sensible**.

Pour elle, le véritable enjeu n’est donc pas seulement technique, mais repose sur une **connaissance globale des données**, leur contexte d’usage, et les personnes qui y accèdent.

D’où sa transition naturelle vers une approche plus large de gouvernance, abordée dans la suite de la conférence.

III. Conditions d'efficacité d'un DLP

Déployer une solution DLP ne garantit pas automatiquement une protection efficace des données sensibles. Comme l'a souligné **Keren Bismuth**, le DLP est un **outil**, pas une baguette magique. Pour qu'il soit réellement utile, il doit s'inscrire dans une **démarche cohérente et structurée**, qui dépasse largement la seule sphère technique.

Elle propose ainsi d'adopter une **vision globale** de la sécurité de l'information, en intégrant les dimensions **organisationnelles, humaines et matérielles** du système d'information.

La donnée peut fuir sous de multiples formes. Si le DLP numérique permet de contrôler les envois via email ou clé USB, il est **impuissant face à certaines fuites physiques** : un écran partagé en visioconférence, une discussion dans un open space, un extrait confidentiel imprimé puis scanné. D'où l'idée forte défendue par l'intervenante : **la meilleure manière de protéger une donnée est d'en limiter l'accès, voire la connaissance**.

Elle propose ainsi de ne pas se concentrer uniquement sur le "transit de la donnée", mais de réfléchir en amont : **qui connaît quoi, à quel moment, et pourquoi ?**

Keren Bismuth propose une méthode simple et efficace, résumée en **trois principes fondateurs** :

Contrôle des accès & vérification des identités

Il s'agit de restreindre l'accès aux seules personnes qui en ont **réellement besoin**.

- Bloquer les **ports USB** non utilisés,
- Restreindre l'usage d'imprimantes à certaines équipes,
- Vérifier l'**utilité réelle** de certains outils métiers.

Exemple : une imprimante accessible à tous peut générer des fuites non tracées. Un accès restreint et guidé permet de réduire ce risque.

Principe du moindre privilège

Ne donner à chaque collaborateur **que les droits strictement nécessaires** à son poste :

- Lecture seule vs modification,
- Accès ponctuel vs accès permanent.

Cela limite les risques de compromission par erreur ou par malveillance. Une fuite est d'autant plus probable que les données sont accessibles de manière large et non maîtrisée.

Micro-segmentation

Ce concept, issu du monde réseau, vise à **contenir les flux de données sensibles** dans des périmètres bien définis, au sein de l'organisation :

- Les données stratégiques ne doivent **circuler qu'entre les entités autorisées**,

- Pas d’accès permanent aux documents confidentiels pour les profils qui n’en ont pas besoin.

Elle rappelle que la **connaissance de la donnée** est déjà un pouvoir : une fuite n’est pas forcément vers l’extérieur, elle peut très bien se produire **en interne**, entre deux équipes non censées partager certains contenus.

Pour illustrer son propos, Keren Bismuth a proposé une image percutante :

"C’est comme une maison équipée de caméras, d’alarmes, de barreaux aux fenêtres… mais dont tout le monde aurait la clé."

La sécurité n’est pas qu’une question de technologie : elle repose sur **des règles d’usage, de cloisonnement, et de contrôle des accès**. Le DLP est une pièce importante du dispositif, mais **c’est toute l’architecture de gouvernance de la donnée** qui doit être pensée de manière cohérente.

IV. Mettre en œuvre un DLP : méthode et gouvernance

La mise en place d'une solution DLP ne se limite pas à un déploiement technique. Pour **Keren Bismuth**, c'est une **démarche progressive, structurée, interdisciplinaire**, qui doit s'appuyer sur une gouvernance solide et une vraie méthodologie. Sans cela, le risque est d'obtenir un outil bridé, sous-exploité, ou générateur de faux positifs.

Plusieurs **acteurs** doivent être impliqués pour garantir le succès d'un projet DLP :

- **Le RSSI** (Responsable de la sécurité des systèmes d'information) : pilote la stratégie de sécurité, initie les campagnes de sensibilisation, définit les règles de détection et choisit l'éditeur de la solution.

- **Le DPO** (Délégué à la protection des données) : intervient sur l'évaluation des risques juridiques en cas de fuite, qualifie les données personnelles, propose ou valide des actions disciplinaires.

- **Les RH** : assurent la sensibilisation des collaborateurs dès leur arrivée, interviennent en cas de rupture de contrat ou d'incident impliquant un salarié.

- **Les métiers / référents DLP** : évaluent les données critiques, construisent les scénarios de fuite, pilotent les règles et assurent l'adaptation continue de la solution aux besoins.

- **L'éditeur de la solution DLP** : acteur externe mais clé, à intégrer dans l'écosystème de gouvernance pour garantir un paramétrage adapté et évolutif.

Parmi tous ces profils, **le référent DLP** (fonction souvent transverse ou rattachée au RSSI) joue un rôle essentiel dans l'opérationnalisation du dispositif. Il est responsable de plusieurs volets:

- **Gestion des accès à la solution** : déterminer qui peut créer, modifier ou consulter les règles de détection.

- **Pilotage des politiques de détection** : maintenir un fichier de suivi des règles DLP (objectif, périmètre, date de mise en œuvre, efficacité, obsolescence…).

- **Intégration avec l'Active Directory** : garantir que l'ensemble des collaborateurs soit bien répertorié et que les alertes DLP puissent leur être associées. Un utilisateur non présent dans l'AD ne pourra pas être surveillé.

Keren Bismuth propose une approche pragmatique en **trois grandes étapes** pour cadrer la mise en œuvre d'un DLP :

Approche par le métier

Chaque entité doit identifier ses données critiques via une **analyse d'impact métier** (BIA – Business Impact Analysis). L'objectif : qualifier la sensibilité des données, documents, projets ou applications selon leur impact en cas de fuite.

💡 Attention : deux équipes classées “confidentielles” peuvent avoir des niveaux de criticité très différents. Il est essentiel d’avoir un système de classification homogène et harmonisé à l’échelle du groupe.

Cartographie des actifs

Un **inventaire exhaustif des systèmes, équipements, serveurs et périphériques** est indispensable pour déployer un DLP pertinent :

- Quels actifs doivent être couverts ?
- Lesquels ne le seront pas, et pourquoi ?
- Quelles données circulent sur quels actifs ?

Cette étape permet aussi d’anticiper les cas de **shadow IT** (actifs non répertoriés et donc non protégés).

Évaluation des risques et conception des règles

Enfin, il faut formaliser des **scénarios de fuite de données** (ex. : envoi d’un fichier RH vers une adresse personnelle) et créer les **règles DLP correspondantes** :

- Que doit détecter la règle ?
- Que ne peut-elle pas détecter ?
- Quelles zones de risque doivent être couvertes autrement ?

Le “gap” entre ce qui est couvert et ce qui ne l’est pas doit être **documenté et assumé** – avec validation par le RSSI ou la gouvernance cyber.

Cette méthode permet de s’assurer que les règles de DLP ne sont pas simplement techniques, mais bien **ancrées dans la réalité des usages et des risques métiers**. Le but n’est pas d’empêcher les utilisateurs de travailler, mais de prévenir intelligemment les fuites, sans générer de friction ni de contournement.

V. Incidents, fuites, et retours d’expérience

Après avoir détaillé la méthodologie de mise en œuvre d’un DLP, **Keren Bismuth** a consacré une partie de son intervention à l’analyse des **incidents** et **types de fuites** les plus fréquemment observés en entreprise. Cette approche très concrète a permis de faire le lien entre la théorie du DLP et les **cas réels** du terrain.

Un **événement** est une alerte déclenchée par une règle DLP. Il devient **incident** lorsqu’une fuite est confirmée. Cette distinction est cruciale pour éviter les faux positifs et adapter les réponses.

Les fuites fréquentes :

- **Fin de contrat** : envois massifs vers une adresse personnelle.
- **Erreurs d’envoi** : mauvaise adresse email ou pièce jointe.
- **Fichiers Excel mal filtrés** : données non visibles mais incluses.
- **Usage personnel** : confusion entre email pro/perso.

Ces situations relèvent souvent d’un **manque de sensibilisation** ou d’une **absence de processus de contrôle**.

Les **incidents** touchent généralement :

- Données personnelles (identité, RIB…),
- Présentations client,
- Guides ou documents internes confidentiels.

En cas d’incident, une **analyse** doit être menée pour qualifier :

- La nature de la donnée,
- Le canal utilisé,
- Les destinataires impliqués,
- Les droits d’accès de l’expéditeur.

Et surtout, ne **pas suggérer de justification** à l’émetteur : il faut recueillir les faits de manière neutre pour éviter toute manipulation involontaire.

VI. Choisir une solution DLP adaptée

Pour conclure sa présentation, **Keren Bismuth** a rappelé qu'une solution DLP n'est jamais "clé en main" : son efficacité dépend largement de sa bonne intégration dans l'environnement technique, humain et organisationnel de l'entreprise. Il ne s'agit pas seulement de comparer des fonctionnalités sur une plaquette commerciale, mais d'identifier ce qui répond réellement aux risques propres à chaque structure.

Avant tout, l'entreprise doit définir ses besoins : souhaite-t-elle que la solution bloque automatiquement les fuites, ou qu'elle se contente de remonter des alertes pour analyse ? Quels canaux doivent être surveillés en priorité : les emails, les périphériques USB, les impressions, les transferts vers le cloud ? Ces arbitrages sont cruciaux car ils influencent à la fois l'ergonomie, la performance et l'acceptation de l'outil par les utilisateurs.

Une attention particulière doit être portée à la **compatibilité de la solution avec l'environnement existant** : systèmes d'exploitation, messageries, services cloud, etc. Certaines solutions intègrent aussi des fonctionnalités avancées comme la suggestion automatique de sensibilité ou la reconnaissance de contenu sensible, mais ce ne sont pas des standards du marché. Ces modules peuvent être utiles, mais ils **ne remplacent pas une stratégie de gouvernance bien construite**.

Keren Bismuth invite enfin à **rester vigilant face aux promesses commerciales**. Certaines solutions se présentent comme **des outils "anti-fuite",** sans répondre pleinement aux enjeux d'un **DLP global**. Parfois, les définitions employées **ne sont pas conformes** à celles utilisées dans les **référentiels métiers ou réglementaires**, ce qui peut créer des malentendus, voire de mauvaises décisions. Le bon choix passe donc par **une analyse rigoureuse des risques**, **une bonne compréhension des fonctionnalités réelles** proposées par l'éditeur, et **une implication forte du RSSI et des métiers dès la phase d'évaluation**.

VII. Intervention du général (2S) Didier Looten

Comme le veut la tradition des *Lundi de la cybersécurité*, une séquence intermédiaire a permis de mettre en lumière une personnalité engagée dans l'écosystème de la cybersécurité. Pour cette édition, c'est le **général (2S) Didier Looten**, **président de l'ARCSI** (Association des Réservistes du Chiffre et de la Sécurité de l'Information), qui a pris la parole.

Ancien officier général de l'armée de l'air et de l'espace, Didier Looten a dédié plus de 40 ans au service des systèmes d'information du ministère des Armées, avant de rejoindre le secteur privé. Il est aujourd'hui directeur cybersécurité chez **Engie**, au sein de la direction Grand Public. Il poursuit également plusieurs engagements bénévoles, notamment à travers la présidence de l'ARCSI.

Lors de son intervention, il a présenté les missions de l'ARCSI, association fondée en 1928 et rassemblant aujourd'hui plus de 300 membres, experts civils et militaires de la cybersécurité, de la cryptologie, du renseignement ou encore du droit du numérique. L'ARCSI mène une veille active, publie régulièrement des contenus techniques, organise des rencontres professionnelles et participe aux grands événements du secteur.

Il a aussi annoncé les prochaines **Rencontres de l'ARCSI**, qui auront lieu le **22 mai 2025 à l'ESIEA (Paris)**, sur le thème : *« 100 ans de mécanique quantique : quelle sécurité pour le cybermonde du XXIe siècle ? »*. Une journée entière de conférences et de tables rondes sera consacrée à la cryptographie post-quantique, un sujet stratégique pour l'avenir de la cybersécurité.

Son intervention a permis de rappeler l'importance du dialogue entre les mondes militaire, académique et industriel, ainsi que le rôle fondamental des communautés expertes pour anticiper les évolutions technologiques à venir.

VIII. Questions / Réponses

Q : Des documents jugés non critiques peuvent-ils, par recoupement, révéler des informations sensibles ?

R : Oui. Le recoupement d'informations non sensibles peut conduire à la reconstitution d'une donnée stratégique. C'est une méthode utilisée par les cyberattaquants, et les entreprises doivent, à leur tour, anticiper ces scénarios.

Q : Est-il possible d'utiliser un DLP pour surveiller les environnements collaboratifs comme Microsoft Teams ?

R : Oui, certains outils comme **Microsoft Purview** permettent de classifier et appliquer des règles de rétention dans des environnements comme Teams, qui sont effectivement de plus en plus concernés par les fuites de données.

Q : Quel budget prévoir en services pour chaque euro investi dans une licence DLP ?

R : Il n'y a pas de règle fixe, mais on peut s'attendre à des coûts en services significativement supérieurs au coût de la licence : intégration, paramétrage, sensibilisation, gouvernance... C'est un projet à forte composante humaine.

Q : Existe-t-il des règles similaires à celle interdisant de faire des recherches identifiables sur Internet, comme cela se pratiquait chez PSA dans les années 1990 ?

R : Oui, la logique reste valable aujourd'hui : il est pertinent de restreindre l'accès aux sites non liés au métier de l'équipe, pour éviter toute fuite involontaire d'information ou d'intention stratégique.

Q : Est-il possible qu'une simple recherche Google expose des informations sensibles à des tiers ?

R : Oui. Une requête, même anodine, peut trahir l'état d'avancement d'un projet. Il est recommandé d'utiliser des moteurs de recherche internes ou anonymisés, surtout pour les grands groupes sensibles.

Q : Faut-il mettre à jour la charte informatique lors du déploiement d'un DLP ?

R : Il est conseillé de s'assurer que la charte couvre bien les aspects liés à la surveillance des usages et à la protection des données. Une **information claire** doit aussi être communiquée aux collaborateurs en amont du déploiement.

Q : Quelles actions de sensibilisation sont nécessaires autour du DLP ?

R : Les bonnes pratiques doivent être adaptées aux métiers (finance, relation client, etc.). Cela inclut l'usage des outils recommandés, la vérification des identités, la prudence sur les réseaux sociaux, et la mise à disposition de canaux internes pour poser ses questions en cas de doute.

Q : La conférence de l'ARCSI du 22 mai à l'ESIEA sera-t-elle accessible à distance ?

R : Oui. Un formulaire d'inscription sera bientôt disponible sur le site de l'ARCSI, permettant de choisir entre **présentiel** et **distanciel**, selon les préférences des participants.