Formations du Conseil Régional

FAD via plateforme Occitanie e-Formation

BAC + 4 MIS
Veille stratégique
Séance cours 2

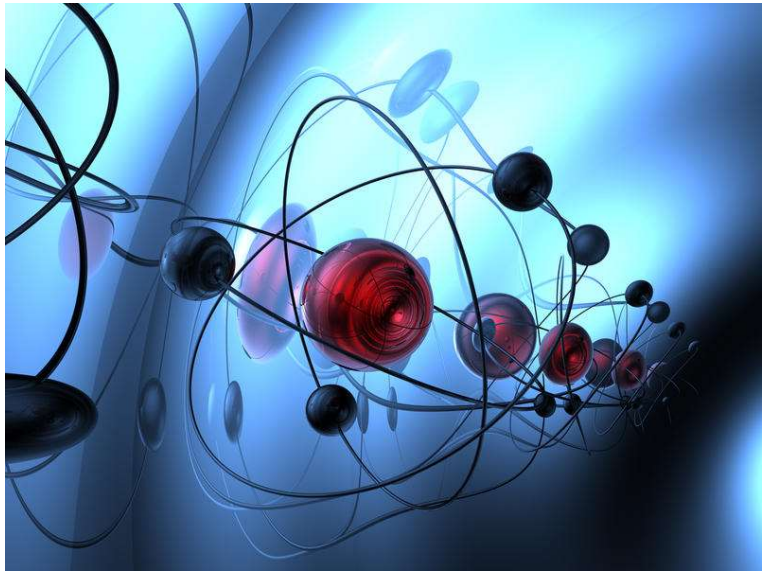
Intervenant : Nicolas Leleu

Agenda des cours

1. Historique et cadre réglementaire / Le renseignement et l'approche moderne du monde digital
2. **Fonctions de l'IE : connaître son environnement concurrentiel (veille), protéger son savoir-faire et influencer**
3. Mise en œuvre d'une démarche structurée et humaine
4. Séance inversée - auto-formation
5. L'identification des informations sensibles, l'information et la sanction
6. L'entreprise et ses menaces, du badge d'accès à la connexion wifi

Agenda du 2e cours

1. **Connaître son environnement concurrentiel (veille)**
2. Protéger son savoir-faire
3. Influencer
4. Divulgation d'informations confidentielles



1 – CONNAITRE SON ENVIRONNEMENT CONCURENTIEL

1.1 – Organiser un dispositif de veille

- La veille est la base de la démarche d'intelligence économique. Elle est indispensable pour développer des stratégies de sécurité et d'influence.
- Consiste à collecter, traiter, hiérarchiser, analyser, valider, mettre en forme et diffuser de manière méthodique des informations rassemblées à partir de nombreuses sources ouvertes et légalement accessibles en utilisant de préférence des compétences pluridisciplinaires.

- Permet d'obtenir des connaissances utiles à partir d'un foisonnement d'informations (importance du management de la connaissance - knowledge management)

- Produire de la connaissance utile :
  - pour se positionner face à l'environnement extérieur et international et devancer la concurrence ;
  - pour s'enrichir des bonnes pratiques d'autres acteurs ;
  - pour réduire l'incertitude.

- Veille technologique, sociétale, juridique, marché, brevets, etc.

1 – CONNAITRE SON ENVIRONNEMENT CONCURENTIEL

1.2 – Anticiper : prévoir les évolutions pour agir en conséquence

- Fondée sur la prévision et la prospective
- Nécessite un capital informationnel régulièrement actualisé par les résultats de la veille
- S'obtient en croisant la connaissance, l'expérience et les résultats de modèles prédictifs.
- Elle apporte une valeur prédictive à la veille.

<u>Comment penser les scenarii de recherche</u> :

- détermination de facteurs critiques généraux à partir du plan stratégique de l'entreprise ;
- sujets techniques ;
- sujets économiques ;
- ruptures de niveau stratégique.

Le succès de la veille et de l'anticipation est étroitement lié à la gestion des ressources humaines de l'entité.

1 – CONNAITRE SON ENVIRONNEMENT CONCURENTIEL

1.3 – Le management de la connaissance

- information formelle et informelle, explicite et implicite, tangible ou tacite ;
- structuration de l'information et de sa mise à jour ;
- importance de la mémoire interne de l'entité pour contribuer à une veille complète ;
- importance des réseaux interne et externe pour s'alimenter en information ;
- organisation des connaissances ;
- diffusion et partage des connaissances pour avoir la bonne information au bon moment ;
- l'intelligence collective ;
- le risque : uniformisation des analyses par l'utilisation d'outils standardisés.

1 – CONNAITRE SON ENVIRONNEMENT CONCURENTIEL

1.4 – Le cycle de l'information

- Expression des besoins,
- Recueil,
- Validation,
- Tri,
- Mise en forme,
- Analyse,
- Diffusion,
- Nouvelle expression des besoins.

<u>Deux modes principaux :</u>

- la veille portant sur un secteur d'activités ou un domaine
- le recueil d'informations portant sur un sujet précis.

1 – CONNAITRE SON ENVIRONNEMENT CONCURENTIEL

1.5 – Comment faire de la veille ?

Multiplier les sources

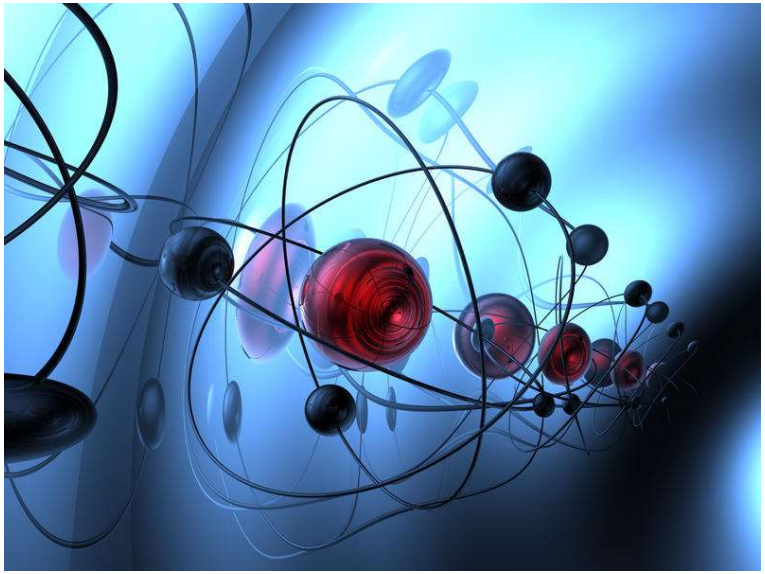
- Utiliser des sources légalement accessibles.
- Organiser le réseau humain de recueil d'informations
- Sélectionner les sources utiles à la veille numérique : notion de qualification et d'indice de fiabilité des sources.
- Croiser les sources, vérifier les informations pertinentes, éviter les désinformations.
- Stocker et classer les données et les informations.

Utiliser tous les outils disponibles

- Gratuits, payants, nécessité d'investir ou pas dans un outil spécifique
- Dits sémantiques (datamining).
- De cartographie.
- De surveillance de l'e-réputation.
- De vérification des contenus et des identités des interlocuteurs.
- De veille furtive, de cartes mentales (mind mapping).

Agenda du 2e cours

1. Connaître son environnement concurrentiel (veille)
2. **Protéger son savoir-faire**
3. Influencer
4. Divulgation d'informations confidentielles



2 – PROTEGER SON SAVOIR-FAIRE

2.1 Définir l'information dites « sensibles »

- Travail à mener de concert avec plusieurs services de l'entreprise

1. les informations techniques et technico-commerciales
2. les informations commerciales

–

3. les informations économiques et financières
4. les informations stratégiques et organisationnelles

➢ Attention : tout n'est pas confidentiel

2 – PROTEGER SON SAVOIR-FAIRE

2.2 Signaler les informations sensibles

- Apposer une mention telle que « confidentiel » sur les documents sensibles (offres, documents techniques, plans…) ainsi que dans les courriers ou courriels qui les accompagnent, complétée d'une clause type spécifiant l'usage restrictif, sous peine d'engager sa responsabilité.

➢ Décrire ces informations dans un accord de confidentialité dès lors que cela est possible.
➢ Le marquage peut s'avérer nécessaire mais n'est pas toujours suffisant

- En interne, il importe de sensibiliser et d'impliquer les salariés.

- En externe, il est recommandé de signer des accords de confidentialité

1. faire figurer la mention « confidentiel » sur les offres, documents techniques et plans,

2. insérer des clauses mentionnant que l'offre et son contenu sont communiqués aux seules fins d'évaluation de l'offre

2 – PROTEGER SON SAVOIR-FAIRE

2.3 Analyse des risques et du préjudice si divulgation

La perte, la destruction ou la divulgation de cette information est-elle de nature à engendrer …	Impact faible	Impact moyen	Impact fort
… un dommage pour l'activité de la structure ou le déroulement d'un projet ?			
… un impact financier ou technique ?			
… un impact sur le personnel ?			
… un impact en matière d'image et de réputation ?			
… une incidence sur la confiance des actionnaires ou des banques ?			
… une perte de confiance d'un client ou d'un partenaire important ?			

- impact fort : protection et traçabilité spécifiques
- impact moyen : analyse supplémentaire du degré d'exposition de ces informations

2 – PROTEGER SON SAVOIR-FAIRE

2.4 Protéger son savoir et ses idées

1. Identifier parmi les différents titres de propriété intellectuelle ceux qui sont les mieux adaptés pour protéger et valoriser ses innovations, ses produits ou ses créations immatérielles.

2. Vérifier auprès de l'institut national de la propriété industrielle (INPI) la disponibilité du droit à protéger (recherches d'antériorité)

3. Identifier les marchés présents et futurs. Se renseigner auprès du réseau d'experts à l'international

4. Enregistrer ses droits auprès des offices compétents.

5. Faire enregistrer les noms de domaine liés aux titres et à l'activité commerciale auprès de l'agence française pour le nommage sur internet en coopération (AFNIC).

2 – PROTEGER SON SAVOIR-FAIRE

2.5 La quête d'informations stratégiques

- Défini aux articles 411-1 et suivants du code pénal, l'espionnage réprime de la manière la plus sévère « Le fait de livrer à une puissance étrangère, à une organisation étrangère ou sous contrôle étranger [...] des documents, matériels, équipements, etc. ».

- De nombreuses affaires à portée internationale ont mis en évidence l'existence de faits d'espionnage industriel sans que la notion d'espionnage ne soit systématiquement retenue par les tribunaux judiciaires. La protection européenne du secret des affaires apporte une réponse nouvelle. Toutefois, la captation malveillante demeure, dans la plupart des cas, liée à des faiblesses humaines ou organisationnelles. Quelle que soit la technique utilisée, c'est bien l'information stratégique de l'entreprise qui est visée.

- Mettre en œuvre l'art de la tromperie et de la persuasion

  ➔ L'art de la tromperie et de la persuasion ne fait qu'exploiter les faiblesses individuelles de chacun avec des conséquences parfois très dommageables pour l'entreprise, quand elles ne se révèlent pas irréversibles !

2 – PROTEGER SON SAVOIR-FAIRE

2.5 La quête d'informations stratégiques

- Avec « MICE », on ne va peut-être pas vous manquer !
  - ➔ Cet acronyme anglo-saxon reprend les quatre leviers de la manipulation que sont l'argent (Money), l'adhésion à une cause (Ideology), le chantage (Compromission) et le besoin de reconnaissance (Ego).

- Préserver les intérêts fondamentaux de la nation
  - ➔ La divulgation d'informations portant atteinte aux intérêts fondamentaux de la nation est réprimée par 15 ans de détention criminelle et 225 000 euros d'amende (Article 411-6 du code pénal)
  - ➔ Les intérêts fondamentaux comprennent le patrimoine culturel et le potentiel économique et scientifique de la France (Article 410-1 du code pénal)

2 – PROTEGER SON SAVOIR-FAIRE

2.5 La quête d'informations stratégiques

- La protection du secret de la défense nationale est visé par l'article 413-9 du code pénal

➔ Le 8 juin 2016, le parlement européen votait définitivement la « directive européenne sur la protection des savoir-faire et des informations commerciales non divulguées » mieux connue sous le vocable de « directive européenne sur le secret des affaires ».

➔ La loi n°2018-670 du 30 juillet 2018, qui en constitue la transposition française, énonce que toute information peut-être protégée au titre du secret des affaires sous réserve :

- Qu'elle ne soit pas connue du grand public ou du secteur d'activité concerné
- Qu'elle revête une valeur commerciale, effective ou potentielle, du fait de son caractère secret
- Qu'elle fasse l'objet de la part de son détenteur légitime de mesures de protection raisonnables pour en conserver le caractère secret

2 – PROTEGER SON SAVOIR-FAIRE

2.6 Utilité des dépôts privés

- Lorsque des informations techniques sont jugées spécialement précieuses ou stratégiques pour l'entreprise, cette dernière a intérêt à :

1. constituer un dossier contenant la description de ces éléments,
2. faire un « dépôt privé », c'est-à-dire un dépôt non réglementé de données.

- Prouver qu'à la « date certaine » du dépôt, l'entreprise détenait bien les informations pour l'établissement de la preuve de l'antériorité.

- Se placer dans une position plus favorable dans le cadre d'un litige.

- Se ménager une preuve de l'ancienneté de la détention permet de continuer à exploiter l'invention malgré l'existence de ce brevet – c'est ce qu'on nomme la « possession personnelle antérieure » en droit français.

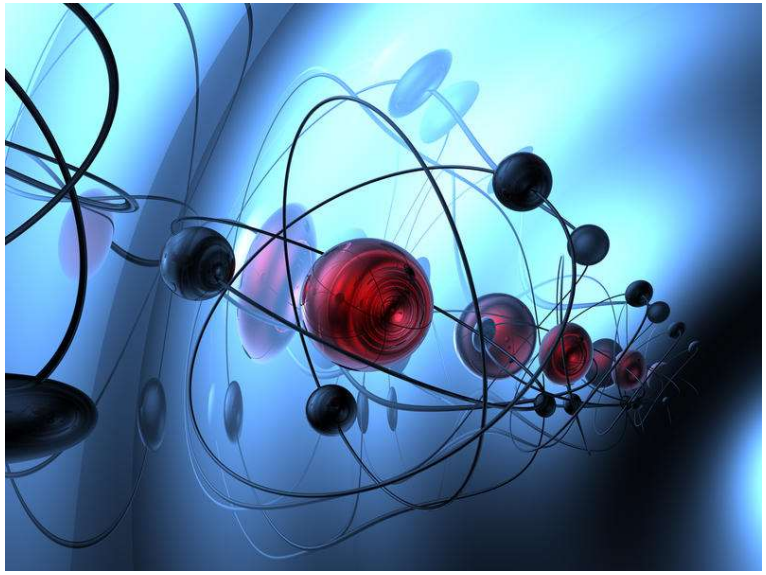
2 – PROTEGER SON SAVOIR-FAIRE

2.7 Les types de dépôts privés

- L'enveloppe Soleau : il s'agit d'une technique française qui permet, par le dépôt de l'enveloppe à l'institut national de la propriété industrielle (INPI),
- Dépôt auprès d'un officier ministériel (huissier ou notaire) dont les actes donnent une date certaine aux dépôts,
- Dépôt en ligne auprès d'un prestataire spécialisé ou de certaines institutions d'ingénieurs. (horodatage et signature électronique, dépôt par un acte d'huissier),
- Envoi d'un courrier recommandé à soi-même,
- L'archivage numérique : preuve légale d'une date de possession d'une information.

Agenda du 2e cours

1. Connaître son environnement concurrentiel (veille)
2. Protéger son savoir-faire
3. **Influencer**
4. Divulgation d'informations confidentielles



3 – INFLUENCER

3.1 – Une démarche hautement stratégique

- L'influence est la capacité à agir sur son environnement de manière à orienter les décisions des acteurs pertinents dans le sens de ses intérêts, de manière légale, sans recours à la contrainte ou à la rémunération.

➢ Repose sur la conviction, l'argumentation, l'exemplarité ou la séduction.

- Les stratégies d'influence visent des objectifs différents selon leurs auteurs :

➢ la puissance (c'est plutôt le cas des États qui souhaitent diminuer l'hostilité à leur égard, multiplier leurs alliés et faire prédominer leur propre vision géopolitique) ;

➢ la domination des marchés (c'est plutôt le cas des entreprises) ;

➢ la prise en compte des idées (c'est plutôt le cas des ONG).

- En France l'influence est professionnelle et utilise des moyens légaux. Mais les outils d'influence ne sont malheureusement pas réservés aux activités légitimes.

3 – INFLUENCER

3.2 – Une nécessaire évolution

- Mais aujourd'hui ces trois objectifs ne sont plus aussi distincts compte tenu des rôles évolutifs des acteurs.

➢ L'influence est une composante des stratégies de puissance, qu'elles se déploient dans le domaine militaire, économique ou culturel.

- Au carrefour d'au moins cinq disciplines :

➢ la psychologie sociale,
➢ la sociologie,
➢ les sciences politiques,
➢ la géopolitique,
➢ les sciences de l'information.

3 – INFLUENCER

3.3 – La maîtrise des outils d'influence

- Démarche indispensable pour consolider un avantage stratégique ou concurrentiel, pour les acteurs publics comme privés, du monde associatif comme du monde académique.

➢ En amont des processus d'influence, de même que les think tanks, producteurs et promoteurs de pensée.

➢ En amont se décline en lobbying, en advocacy, en diplomatie économique, en diplomatie d'entreprise, en soft power, en smart power et en public diplomacy.

➢ Se concrétisent souvent en règles de conformité qu'il s'agit d'anticiper «proactivement»

3 – INFLUENCER

3.4 – Ingénierie d'influence : anticipation, suivi, coopération, travail, alliances

- <u>Élaborer une stratégie d'influence :</u>
  - créer une position et l'argumenter solidement - définir des objectifs et un message ;
  - identifier les cibles, les relais d'opinion, les influences concurrentes ;
  - créer des partenariats ;
  - notion de « coopétition ».

- <u>Persuasion :</u>
  - maîtriser la diffusion de l'information à l'extérieur ;
  - être crédible ;
  - utiliser les réseaux et jeux d'alliances - cartographier les réseaux - faire vivre un réseau ;
  - investir les lieux d'influence et d'opinion ;
  - être en alerte et actif dans les lieux de contrôle et de régulation.

➔ Contre-influence

3 – INFLUENCER

3.5 – Acteurs

États : diplomatie économique, négociations internationales, aide au développement, coopération technique, utilisation des systèmes juridiques, normes de gouvernance mondiale.

- action opérationnelle pour promouvoir ses valeurs et ses intérêts ;
- attraction des capitaux étrangers ;
- soutien de la présence internationale d'entreprises.

Entreprises et associations professionnelles : lobbying, advocacy, partenariats, coalitions

- actions à destination des décideurs politiques ;
- actions envers le grand public ;
- action sur les champs de la normalisation et de la standardisation ;
- action sur l'image de l'entreprise ;
- transfert des innovations académiques vers le tissu industriel ;
- gestion de la crise de réputation.

Société civile : ONG, groupements professionnels, notamment internationaux, think tanks

- agir sur les idées et les opinions
- les publications
- l'opinion publique internationale.

3 – INFLUENCER

3.6 – PERSUADER OU MANIPULER ?

- L'ANSSI définit l'ingénierie sociale comme une

  « ***manipulation consistant à obtenir un bien ou une information, en exploitant la confiance, l'ignorance ou la crédulité de tierces personnes*** ».

- Approche à la fois psychologique et systémique, l'ingénierie sociale permet à des personnes malintentionnées de ***manipuler un individu, en vue d'obtenir de sa part des informations stratégiques ou des comportements inadaptés***.

- Constituant l'un des moyens les plus exploités par les auteurs d'escroqueries économiques et financières pour parvenir à leurs fins, sociale fragilise chaque année de nombreuses entreprises, quand elle tout simplement leur perte.

- Les personnes physiques qui en sont victimes subissent un réel traumatisme qu'elles ont beaucoup de mal à surmonter.

3 – INFLUENCER

3.7 – DES ATOUTS POUR CONVAINCRE

- Technique de communication par nature intrusive, l'***ingénierie sociale n'est pas pour autant illégale***.
- Dans la plupart des cas, elle s'appuie sur une étude préalable des environnements personnel et professionnel de la future victime. La personne malintentionnée cherchera alors à établir dans un premier temps une relation de confiance avant d'entrer ensuite en ***contact direct*** avec son interlocuteur, soit par ***médias sociaux*** interposés, soit par ***courrier électronique***, soit par ***téléphone***. Même si elle expose son auteur à davantage de risques, la recherche d'une relation directe par contact physique ne doit pas être écartée.

- Dans son rapport sur l'état de la menace lié au numérique pour l'année 2018, le délégué ministériel aux industries de sécurité et à la lutte contre les cybermenaces (DMISC) rappelle que les techniques d'ingénierie sociale et les vulnérabilités résiduelles touchent une entreprise sur deux !

3 – INFLUENCER

3.8 – FAUX PRÉSIDENT, FAUX VIREMENT, MAIS VRAIE ESCROQUERIE !

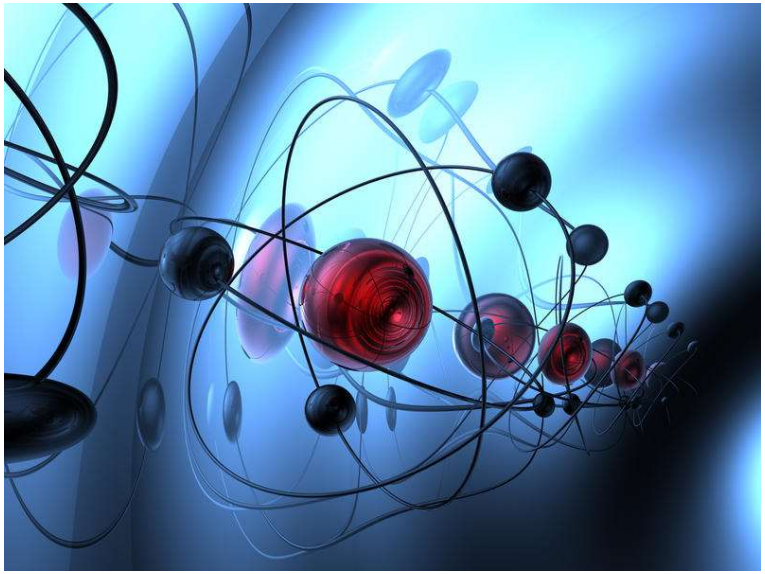
- L'ingénierie sociale permet, à ceux qui en exploitent les ressorts et les ressources, de commettre des escroqueries toujours plus sophistiquées. Pourtant, dans la majeure partie des cas, les fraudeurs ***exploitent une faille humaine et des faiblesses organisationnelles***.

- A titre d'exemple, l'escroquerie dite des faux ordres de virement internationaux ou du faux président, vise à obtenir par des moyens frauduleux (faux nom ou fausse qualité, mise en scène, etc.) la remise de fonds par virement bancaire.

- Quelques mesures simples suffisent parfois à réduire les risques :
  - Toujours vérifier l'identité de son interlocuteur par un rappel sur des coordonnées identifiées,
  - Vérifier systématiquement l'adresse courriel de son correspondant,
  - Instaurer une procédure de séparation des pouvoirs en matière de saisie et de validation,
  - Exclure les paiements de fin de semaine afin être en mesure de réagir rapidement auprès des banques en cas d'atteinte avérée, etc.

Agenda du 2e cours

1. Connaître son environnement concurrentiel (veille)
2. Protéger son savoir-faire
3. Influencer
4. **Divulgation d'informations confidentielles**



4 - DIVULGATION D'INFORMATIONS CONFIDENTIELLES

4.1 SENSIBILISER ET IMPLIQUER

- Impératif de sensibiliser et d'impliquer le personnel de tous les services de l'entreprise, et plus particulièrement lorsqu'ils ont accès à des informations sensibles.

➢ Le personnel doit avoir conscience de ce qui est confidentiel ;

➢ La vigilance doit aussi s'exercer à l'égard des informations confidentielles reçues ;

➢ Les ingénieurs, techniciens et décideurs notamment, doivent être conscients de la valeur des informations qu'ils créent et des informations en leur possession ;

4 - DIVULGATION D'INFORMATIONS CONFIDENTIELLES

4.2 Mesures de restriction

➔ peuvent être prévues concernant la diffusion de certaines informations en interne et/ou à destination d'interlocuteurs extérieurs.

Qui a « besoin d'en connaître » ?

- Liste des personnes habilitées à connaître de telles informations ;
- Imaginer la mise en œuvre d'une protection renforcée par application d'une procédure.

- **En matière de secret défense** : « nécessité impérieuse de prendre connaissance d'une information dans le cadre d'une fonction déterminée pour la bonne exécution d'une mission précise »

- toute personne ne pourra accéder à une information sensible que si sa hiérarchie estime qu'elle remplit la condition du besoin d'en connaître
- seules les personnes habilitées connaissent l'ensemble du dossier
- permet de limiter les risques de divulgation d'une information sensible, que celle-ci résulte d'une inattention ou de l'exercice d'une contrainte.

4 - DIVULGATION D'INFORMATIONS CONFIDENTIELLES

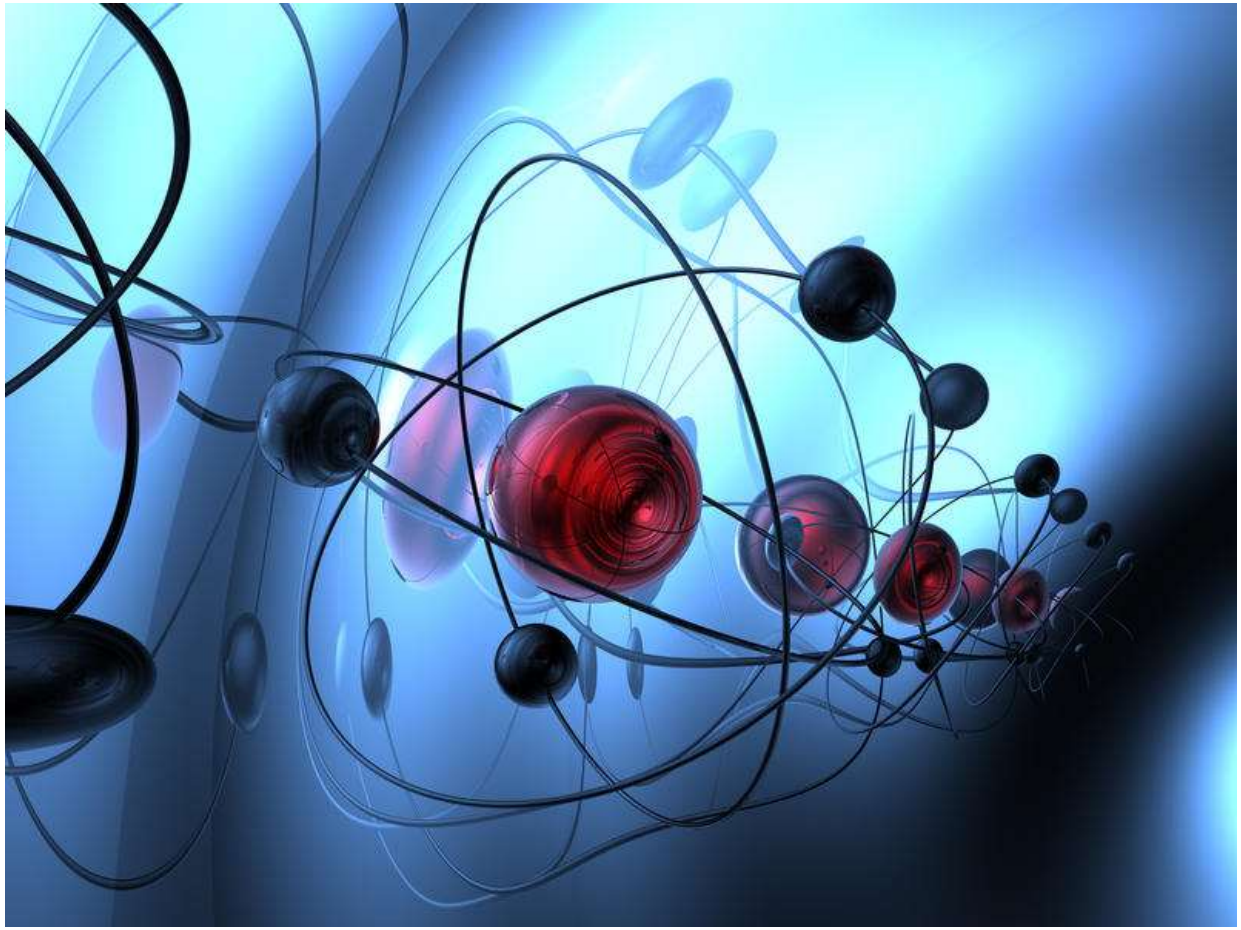
4.3 Une réponse pénale adaptée

- Pour les destructions relevant du droit commun : L'article 322-1 du Code pénal, dispose que « La destruction, la dégradation ou la détérioration d'un bien appartenant à autrui est punie de deux ans d'emprisonnement et de 30 000 euros d'amende, sauf s'il n'en est résulté qu'un dommage léger ».

- Pour les destructions visant les intérêts fondamentaux de la nation : L'article 411-9 du Code pénal réprime beaucoup plus sévèrement les destructions lorsque ces faits sont de nature à porter atteinte aux intérêts fondamentaux de la nation. Les peines prévues vont de 15 à 20 ans de détention criminelle et l'amende peut atteindre 300 000 euros.

- Pour la faute lourde du salarié : Dans le cadre des relations de travail, la faute lourde constitue la faute la plus sévère qui puisse être relevée à l'encontre d'un salarié, en ce sens qu'elle révèle une intention de nuire vis-vis de son employeur ou de l'entreprise concernée.

Questions ?



Fin du 2e cours

BAC + 4

Veille stratégique

Intervenant : nleleu@guartor.com