Paris, le 21 décembre 2012

Note à l'attention de

Mesdames et Messieurs
les Directeurs d'Unité

Le Président

www.cnrs.fr

Campus Gérard-Mégie
3, rue Michel-Ange
75794 Paris cedex 16

T. 01 44 96 40 00
F. 01 44 96 49 13

Dossier suivi par Louis Di Benedetto
05 62 24 25 22 16 / Louis.DIBENEDETTO@dsi.cnrs.fr

Réf. : NOT15YDSI-RSSIC

Objet : sécurisation des ordinateurs

La recrudescence des vols d'ordinateurs - mise en évidence par l'augmentation des signalements qui me remontent - me conduit à vous alerter à nouveau sur la nécessité de mettre en œuvre les mesures de protection adaptées aux enjeux de notre organisme.

Les matériels volés ne sont pas toujours protégés par chiffrement comme demandé dans ma note du 16 janvier 2011 (réf. Not11Y159DSI), les voleurs peuvent alors très facilement accéder aux données stockées.

Ces vols sont susceptibles de remettre en cause la confiance que nous portent nos partenaires industriels et dégrader l'image de marque des unités touchées. Ils peuvent également réduire à néant nos efforts de recherche : perte des données de recherche, vol d'informations par des équipes concurrentes, par des sociétés tierces, revente de données à des organisations mafieuses, etc. *In fine,* ces vols pourraient même avoir des conséquences juridiques importantes pour le CNRS.

Or, le directeur d'unité est responsable de la sécurité des systèmes d'information au niveau de son unité. Conformément à la décision DEC111261DAJ du 12/09/2011, sa responsabilité peut, à ce titre, être recherchée au plan juridique (cf. fiche n°1 en annexe).

Ces risques sont réels. En octobre, nous avons encore dû saisir la justice pour le vol ciblé de l'ordinateur d'un chercheur (non chiffré, dernière sauvegarde en septembre) alors que l'instruction du dépôt de brevet devait débuter, en lien avec trois partenaires industriels majeurs.

Aussi j'attire de nouveau votre attention sur les deux principes qui permettent de réduire les risques liés au vol d'ordinateur et que je vous demande de mettre en œuvre :

- **La protection technique du poste et de ses périphériques de stockage** (cf. fiche n°2 en annexe) :
  - Par le chiffrement du poste de travail et des périphériques de stockage (clé USB, disque externe) ;
  - Par la sauvegarde régulière du poste de travail (localement pour l'instant, une solution nationale étant à l'étude)
- **La sensibilisation du personnel** (cf. fiche n°3 en annexe) :
  - au risque de vol
  - aux conséquences potentielles en fonction de la nature des données volées
  - aux bonnes pratiques permettant de limiter les risques.

Le marché national passé par le CNRS avec la société DELL permet d'acheter des PC portables dont le disque dur est chiffré de façon native. A compter de la parution de cette note, tout nouveau PC portable doit être acheté, quel que soit l'origine des fonds, via ce marché national avec l'option disque chiffrant (cf. fiche n°4 en annexe).

Pour les ordinateurs Mac et Linux, le chiffrement du disque doit être activé via le logiciel fourni en natif sur toutes les machines (cf. fiche n° 2 en annexe).

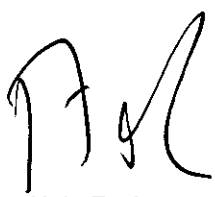
Le déploiement du chiffrement doit être réalisé sur l'ensemble des postes de travail des unités d'ici au 30 juin 2013. À cet effet, les directeurs d'unité transmettront tous les deux mois, via le RSSI de la Délégation Régionale, au directeur général délégué aux ressources, l'état d'avancement de ce déploiement dans leur unité (cf. fiche n°5 en annexe).

Par ailleurs, les RSSI des Délégations Régionales organiseront, en lien avec les Chargés de la SSI des unités, la sensibilisation des personnels et la diffusion des informations techniques à l'adresse du personnel chargé de l'informatique.

Ils rappelleront notamment l'obligation, pour le personnel, et quelles que soient les circonstances du vol, d'avoir à déclarer la disparition de son ordinateur à son Directeur d'unité qui en informera alors le Délégué régional. Le Délégué régional en rendra compte sans délai au RSSI du CNRS, au Directeur des affaires juridiques ainsi qu'au Fonctionnaire de sécurité

Ils rappelleront notamment l'obligation, pour le personnel, et quelles que soient les circonstances du vol, d'avoir à déclarer la disparition de son ordinateur à son Directeur d'unité qui en informera alors le Délégué régional. Le Délégué régional en rendra compte sans délai au RSSI du CNRS, au Directeur des affaires juridiques ainsi qu'au Fonctionnaire de sécurité défense, et portera plainte conformément au paragraphe II.2 de circulaire 80001/DAJ du 21 juillet 2008 (fiche 6 en annexe).

Je vous demande de diffuser cette note auprès de vos personnels et de veiller à l'application des directives dans les délais impartis.



Alain Fuchs

Copie :
- Messieurs les Délégués Régionaux
- Monsieur le Directeur général délégué à la science
- Mesdames et Messieurs les Directeurs d'institut

Fiche n°1 : Exemple de la mise en jeu de responsabilités pour défaut de chiffrement

Les mécanismes de la mise en jeu de responsabilités pour défaut de chiffrement

Lors d'un déplacement, un chercheur du CNRS est victime, dans un lieu public, du vol de son sac contenant notamment l'ordinateur portable lui a mis à disposition par l'établissement pour l'exercice de ses activités professionnelles. Une plainte est déposée au service de police, le voleur et l'ordinateur ne sont pas retrouvés.

A partir de cette situation, une succession de mise en jeu de responsabilités se déclenche, celle de l'agent, du directeur d'unité et du CNRS, personne morale représentée par le président. Les données professionnelles contenues dans l'ordinateur portable vont être à l'origine de réclamations en réparation de préjudice.

Après l'analyse du contenu du portable (dont on ne connait pas le sort fait par le malfaiteur), il est constaté qu'il contient des données extrêmement sensibles, notamment la totalité des résultats de recherche issus d'un contrat de partenariat avec un groupe industriel, en cours de procédure de dépôt d'une demande de brevet

S'il apparaît à cette occasion que le contenu de l'ordinateur portable n'a pas été chiffré, la responsabilité du chercheur, de son directeur d'unité et du CNRS risquent alors d'être mises en cause :

- **La responsabilité personnelle du chercheur :**

Le partenaire industriel peut former un recours devant le juge civil, pour **obtenir réparation du préjudice financier et de la perte d'avantage concurrentiel** subis. Il peut mettre en avant **la faute du chercheur**, qui, en ne chiffrant pas le contenu de son ordinateur portable, n'a pas respecté les obligations de confidentialité prévues par le contrat de partenariat passé avec le CNRS. **La responsabilité personnelle du chercheur, pourtant victime du vol peut ainsi être engagée.**

- **La responsabilité personnelle du directeur d'unité :**

S'il n'a reçu aucune instruction pour chiffrer son portable, **le chercheur pourra à son tour mettre en cause la responsabilité personnelle de son directeur d'unité**, en charge de la sécurité des systèmes d'information au sein de l'unité, qu'il dirige.

Si le **directeur d'unité ne peut apporter la preuve** qu'il avait pris les mesures nécessaires pour chiffrer les portables de l'unité, **sa responsabilité personnelle peut finalement être retenue**, avec toutes les conséquences financières associées.

- **La responsabilité du CNRS, personne morale :**

Le CNRS peut également être mis en cause, car c'est bien l'organisme, comme personne morale, qui a signé le contrat de partenariat qui incluait des clauses de confidentialité.

Pour éviter la mise en cause en cascade des responsabilités et protéger les agents du CNRS et le CNRS, il est donc indispensable de prendre toutes les mesures nécessaires pour chiffrer les ordinateurs portables et éviter ainsi qu'un simple vol ait des conséquences extrêmement lourdes pour les chercheurs et l'Institution.

Fiche n°2 : Protection du poste de travail et des périphériques de stockage

Sauvegardes

- Il est impératif d'effectuer des sauvegardes régulières
  - Un dysfonctionnement matériel ou logiciel peut conduire à la perte d'informations
  - Une erreur de manipulation peut conduire à un effacement malencontreux
  - Un logiciel malveillant (virus) peut supprimer des données
  - Le matériel peut être volé ou perdu
- Toute information qui n'est pas présente en au moins deux endroits différents et/ou pouvant être détruite par un même évènement (feu, acte malveillant, surtension électrique) doit être considérée comme n'existant pas
- Si une sauvegarde est externalisée (bande stockée à l'extérieur, copie quelque part dans le « cloud » en attendant une solution interne) elle doit être chiffrée avec une clé sous le contrôle exclusif du laboratoire
- Le coût des moyens de sauvegardes doit être intégré dans tout achat d'équipement ou de solution informatique
- Le laboratoire met en place les moyens et outils de sauvegarde adaptés à son environnement (une solution nationale est en cours d'étude)

Chiffrement

Chiffrement du poste de travail

- Il est impératif de chiffrer les données à l'aide d'un dispositif logiciel ou matériel, contrôlé par un mot de passe créé par l'utilisateur lui-même (il doit pouvoir le mémoriser facilement) pour cet usage spécifique et ce mot de passe doit être suffisamment robuste, c'est-à-dire constitué d'un mélange aléatoire de minuscules, majuscules, chiffres et caractères spéciaux et dont la taille minimum dépendra du mécanisme de chiffrement utilisé [1]:
  - Chiffrement matériel (sur DELL) : 8 caractères minimum
  - Chiffrement logiciel (Mac, Linux, TrueCrypt sous Windows) : 12 caractères minimum

- Il faut impérativement effectuer un séquestre des mots de passe (stockage en lieu sûr) afin de pouvoir en assurer le recouvrement en cas d'oubli ou d'indisponibilité de son détenteur
- Le disque (HD ou SSD) des ordinateurs portables doit être chiffré intégralement.

[1] Avec ces caractéristiques, compte tenu des moyens à la disposition de tout à chacun au moment de la rédaction de ce document, le mot de passe ne pourra en général être découvert par une attaque classique en moins d'un an.

- **Les solutions efficaces mais en même temps peu contraignantes à l'usage pour l'utilisateur sont rappelées ci-dessous :**

	Chiffrement matériel du disque (avantage : un seul mot de passe pour ouvrir Windows et déchiffrer le disque)	Chiffrement TRUECRYPT sous **Windows**	Chiffrement logiciel fourni avec **MacOS (même avantage que pour chiffrement matériel du disque**	Chiffrement logiciel fourni avec **Linux (même avantage que pour chiffrement matériel du disque**
Portable DELL disque dur	**Option disque chiffrant au marché Dell (cf. fiche n°5)**	Possible	-	Possible
Portable DELL disque SSD	*Option en cours de négociation avec DELL*	**Possible**	-	**Possible**
PC fixe HP	*Option non disponible actuellement*	**Possible**	-	**Possible**
Mac	-	-	**Possible**	-

Chiffrement des supports amovibles

- Les supports amovibles (clés USB, CD, DVD, disques, carte SD, etc.) doivent être chiffrés s'ils contiennent la moindre information confidentielle
- Le chiffrement peut être réalisé par logiciel pour l'ensemble des supports (clés USB, CD, DVD, disques, carte SD, etc.).
    - **Les logiciels de chiffrement fournis avec les clés USB n'offrent aucune garantie et ne doivent pas être utilisés**,
    - il faut utiliser **le logiciel TRUECRYPT** ou bien le chiffrement fourni de façon native par l'OS :

	Windows	**MacOS**	**Linux**
Logiciel TrueCrypt	**Oui**	**Oui**	**Oui**
Bitlocker (Windows 7)	**Oui**	Non	Non
Filevault (MacOS X)	Non	**Oui**	Non
DM crypt (Linux)	Non	Non	**Oui**

- **Les clés USB avec chiffrement matériel mais dont le mot de passe doit être saisi au clavier de l'ordinateur sont déconseillées.** Seules les **clés USB chiffrées intégrant un clavier** pour entrer le code (par exemple roue crantée) présentent une alternative intéressante (facilité d'utilisation) au

chiffrement logiciel - quelques modèles : Corsair Flash Padlock 2, iStorage Datashur - mais attention, **ces matériels ne sont pas certifiés et ne doivent donc pas être utilisés pour protéger des informations sensibles justifiables d'une protection renforcée** (cf.infra).

Limites du chiffrement et précautions à prendre

- Le chiffrement ne protège plus une information qui a été déchiffrée pour y accéder par son détenteur légitime
    - Faire attention aux regards indiscrets (filtre de confidentialité sur l'écran)
    - Protéger les documents imprimés
    - Mettre en œuvre les bonnes pratiques de sécurisation du poste de travail pour se protéger de codes malveillants qui exfiltreraient des données
- ***Le chiffrement ne protège plus une information lorsque la clé de chiffrement a été compromise*** (divulguée de façon volontaire ou involontaire à un tiers)
    - Faire attention aux regards indiscrets lorsque l'on tape sa clé, surtout dans les transports
    - Ne pas garder sur soi la clé de chiffrement, elle pourrait être volée en même temps que le portable qu'elle est censée protéger
- Mettre en œuvre les bonnes pratiques de sécurisation du poste de travail (anti-virus, etc.) pour se protéger de codes malveillants
- Les informations particulièrement sensibles ne devraient jamais être stockées et traitées ailleurs que dans des endroits sécurisés
- **Les voyages à l'étranger demandent des précautions supplémentaires** (cf. infra *Passeport de conseils aux voyageurs* conseils aux voyageurs

Dispositions particulières concernant les informations sensibles justifiables d'une protection renforcée

- Le chiffrement de données particulièrement sensibles peut justifier, en plus du chiffrement de l'ensemble du disque, d'une couche supplémentaire de chiffrement logiciel par des moyens certifiés par l'ANSSI (cf. infra *Chiffrement de portables mise en œuvre et utilisation).* Dans les cas spécifiques de données très sensibles ou dans des contextes de partenariats externes, le recours à d'autres produits qualifiés par l'ANSSI, pour chiffrer des postes, des clés USB ou des transmissions par mail peut être envisagé.
- **Le traitement et la protection des données classifiées de défense relève de situations exceptionnelles régies par des dispositions spécifiques qui ne sont pas traitées dans cette note.**

Références

Note à l'attention des Directeurs d'Unité sur la protection des ordinateurs portables : http://www.dsi.cnrs.fr/services/securite/Documents/Not11Y159DSI.pdf

Chiffrement de portables mise en œuvre et utilisation : http://www.dsi.cnrs.fr/services/securite/Documents/manuel.pdf

Passeport de conseils aux voyageurs : http://www.securite-informatique.gouv.fr/IMG/pdf/Passeport-de-conseils-aux-voyageurs_janvier-2010.pdf

IGI 1300 - Arrêté du 30 novembre 2011 portant approbation de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000024892134

Fiche n°3 : Sensibilisation aux conséquences d'un vol et mesures de prévention

Cela n'arrive pas qu'aux autres !

Conséquences d'un vol

- Perte de l'outil de travail
- Utilisation du matériel à des fins malveillantes (avec notamment l'utilisation des codes d'accès qui y sont stockés)
- Risque de divulgation d'informations confidentielles avec :
    - Impacts juridiques pour les informations que la loi, un règlement, un contrat impose de protéger (données à caractère personnel, données médicales, secret défense, clauses de non divulgation, etc.)
    - Dégradation de l'image de l'organisation (diffusion sur Internet d'informations qui auraient dû rester secrètes)
    - Perte de compétitivité (divulgation prématurée de résultats de recherches)
    - Pertes financières (perte d'un brevet, d'un contrat)
    - Perte de crédibilité, de capacité à négocier de nouveaux contrats

Mesures de prévention

Dans les locaux de l'unité : compliquer la tâche d'un éventuel voleur

- Fermer à clé la porte de son bureau
- Attacher l'ordinateur avec un câble
- Ranger dans une armoire fermée à clé

En déplacement : être vigilant

- Nombre de disparitions d'ordinateur résultent d'un simple oubli
- Quelques techniques utilisées par les voleurs
    - Profiter dans un train du fait que la personne réponde à un appel téléphonique à l'extrémité du wagon pour lui subtiliser son ordinateur qui est resté sur la tablette
    - Remplacer le bagage contenant l'ordinateur par un autre
    - Profiter de l'absence temporaire du propriétaire dans la pièce pour y subtiliser l'ordinateur
    - Usage de la violence → ne pas résister
- Utiliser un filtre de protection pour éviter les regards des curieux
- Mettre un signe distinctif sur l'appareil et sa housse pour le surveiller plus facilement et éviter les échanges
- Ne pas laisser son matériel en vue (dans une voiture par exemple)

Limiter les conséquences d'un vol éventuel

- Sauvegarder régulièrement
    - Mettre la sauvegarde dans un lieu différent
    - Ne pas transporter la sauvegarde avec l'ordinateur (on a toutes les chances qu'elle soit volée en même temps)
- Verrouiller son ordinateur ou mieux le mettre en veille permanente ou l'arrêter lorsque l'on ne l'utilise plus momentanément
- Chiffrer le disque de son ordinateur

Se préparer à gérer un vol éventuel

- Avoir un inventaire du matériel avec les marques, modèle, numéro de série, adresse MAC de l'interface filaire et Wifi
    - Une astuce, faire une photocopie ou numérisation du dessous de la machine pour avoir les différentes références
- Avoir les coordonnées des personnes à contacter pour faire bloquer les différents comptes utilisés

Références

Passeport de conseils aux voyageurs :
http://www.securite-informatique.gouv.fr/IMG/pdf/Passeport-de-conseils-aux-voyageurs_janvier-2010.pdf

Fiche n°4 : Achat d'ordinateurs

Marché MATINFO II

Le marché informatique passé par le CNRS est divisé en quatre lots :

1) Lot numéro 1 : Micro-ordinateurs compatibles PC dont le titulaire est la société HP
2) **Lot numéro 2 : Micro-ordinateurs portables compatibles PC dont le titulaire est la société DELL**
3) Lot numéro 3 : Micro-ordinateurs de bureau, micro-ordinateurs et serveurs compatibles MAC OS dont le titulaire est France Système
4) Lot numéro 4 : Serveurs dont le titulaire est la société DELL

Ce marché représente un volume d'affaires annuel d'environ 40 millions d'euros dont la moitié concerne des besoins CNRS. Il est passé en groupement avec 5 universités et 7 EPST, le CNRS assurant la coordination pour le compte du groupement.

L'objectif de ce marché est d'offrir le plus vaste choix possible pour les chercheurs et répondre aux besoins par des configurations personnalisables. Ce marché est passé pour une année et renouvelable 3 fois, il a débuté le 1er juillet 2009.

La DDAI prépare dès à présent le dossier pour le nouveau marché, De plus en plus d'universités souhaitent rejoindre le groupement et bénéficier des avantages tarifaires. Les conditions commerciales s'améliorent d'année en année, les prix des matériels diminuent et le niveau de qualité (service après-vente, délais de livraison, facilité d'intégrer l'option disque chiffrant, élargissement des types de disques pouvant être commandés avec l'option disque chiffrant ...) est constaté au niveau des utilisateurs.

Sauf cas exceptionnel, il est obligatoire de passer par ce marché national et de respecter la politique d'achat dans le cadre de l'utilisation des crédits du CNRS.

Marché MATINFO II et chiffrement pour les ordinateurs portables

Le CNRS a conclu un marché national avec la société Dell pour l'achat d'ordinateurs portables de type PC (Windows et Linux). Il est impératif de passer par ce marché pour tout achat d'ordinateur portable dans le cadre de l'utilisation des crédits CNRS.

Il faut systématiquement choisir l'option « **disque chiffré** ». Le surcoût 18€ pour un disque de 320 Go par rapport à un disque de 250 Go est négligeable, surtout pour un disque dont la capacité est 20% plus grande et qui est 30% plus rapide.

Les disques SSD (mémoire flash) sont progressivement inclus dans ce marché, un chiffrement logiciel (TrueCrypt) permet d'attendre l'élargissement de l'offre.

Il faut aussi systématiquement choisir l'option « **Conserver votre disque dur** ». Le surcoût est faible (environ 5€). En cas de panne partielle ou totale, il n'est alors plus nécessaire de retourner le disque au constructeur avec des risques éventuels de divulgation d'informations.

Il faut toujours prévoir un câble pour attacher l'ordinateur afin de rendre plus difficile un vol éventuel. Il est possible de le commander avec l'ordinateur ou d'effectuer un achat auprès de l'UGAP (moins cher).

Commande

Quelques points à prendre en compte lors de la commande :

- Se connecter sur le site : https://dell.quadrem.net/buy/fr/
- S'authentifier en fournissant son email et son mot de passe (la première fois cliquer sur « Inscription »
- Choisir un modèle et cliquer sur « *Configuration »*
- Dans la rubrique « *Disque dur principal* » sélectionner un modèle de **disque chiffré**, exemple : « *Passage au disque dur **chiffré** 320 Go 7200 tr/min +17.00 »*
- Dans la rubrique « ***Conserver votre disque dur*** » cocher la case correspondant à la durée de la garantie.
- Si on ne dispose pas de câble pour attacher l'ordinateur et que l'on ne souhaite pas effectuer un achat auprès de l'UGAP, dans la rubrique « *Accessoires* » cocher la case « ***Câble de sécurité*** ».

Fiche n°5 : Plan de déploiement de la protection sur les ordinateurs

Définition

- Le plan de déploiement a pour but de définir le périmètre à protéger et de fixer des échéances pour le traitement de ce périmètre
- Le traitement comprend la sauvegarde (protection contre la perte de données) et le chiffrement (protection contre la divulgation d'informations confidentielles)
- Le plan de déploiement est validé par le directeur d'unité.

Plan de déploiement

Points à prendre en compte

- Lors de chaque renouvellement de matériel **prévoir systématiquement la mise en œuvre du chiffrement,** donc pour les PC achat via le marché national avec l'option disque chiffrant, pour les MAC mise en œuvre du chiffrement dès la première utilisation
- Prévoir de traiter en priorité :
    - Les ordinateurs portables
    - Les ordinateurs les plus sensibles (forte concentration de données confidentielles, données particulièrement recherchées par la concurrence)
    - Les ordinateurs les plus exposés (déplacements, bureaux non fermés, etc.)

Suivi du déploiement du chiffrement

- Le déploiement est suivi au niveau national par le réseau SSI (Chargés de la SSI dans les unités, RSSI de DR, RSSI du CNRS) qui transmet une synthèse au DGD-R (cf. formulaire de suivi page suivante)
- Le formulaire de suivi doit être transmis au RSSI de la DR, les coordonnées des RSSI sont accessibles ici : https://aresu.dsi.cnrs.fr/spip.php?article46

Formulaire de suivi du déploiement du chiffrement sur les ordinateurs utilisés par le personnel de l'unité

Identification de l'unité

N° de la DR	Nom de l'unité	N°LABINTEL

Nom du directeur de l'unité	Nom du Chargé de la SSI de l'unité

Etat des lieux

Date de l'état des lieux

Nombre d'ordinateurs portables de l'unité	Nombre d'ordinateurs portables chiffrés

Nombre d'ordinateurs fixes de l'unité	Nombre d'ordinateurs fixes chiffrés

CENTRE NATIONAL
DE LA RECHERCHE
SCIENTIFIQUE

Circulaire n°080001DAJ relative à la mise en oeuvre de poursuites pénales par le CNRS

Les atteintes portées aux biens matériels et immatériels et à l'image du CNRS méritent une attention et une vigilance particulière.

La protection du CNRS contre des actes de vol, d'intrusion, de destruction, de dégradation, de piratage, de propos diffamatoires, ... justifie des poursuites pénales à l'encontre des auteurs présumés ou potentiels de ces actes délictueux.

L'objet de la présente circulaire est de rappeler les mesures à prendre et les circuits décisionnels à respecter pour permettre à l'établissement de faire cesser le trouble et obtenir réparation de son préjudice devant la juridiction pénale.

Après un rappel de quelques éléments de procédure pénale utiles **(I)**, seront précisés les acteurs du déclenchement des poursuites au CNRS **(II)** et les modalités du suivi de la procédure judiciaire **(III)**.

I- LES ETAPES DE LA PROCEDURE PENALE [1]

Les principales étapes de la procédure pénale sur dépôt de plainte sont :

- l'information du procureur de la République (plainte),
- la phase d'enquête,
- la décision de poursuite,
- le jugement.

I.1 – L'information du procureur de la République

La plainte est l'acte par lequel une personne (morale ou physique) informe le procureur de la République de la commission d'une infraction (contravention, délit, crime) dont elle a été victime. Il existe deux types de plainte :

■ La plainte simple : Les agents de police judiciaire[2] ont l'obligation de recevoir toute plainte et de la transmettre au service ou à l'unité de police judiciaire compétent (*• art. 15-3 du code de procédure pénale - CPP).*

■ La plainte avec constitution de partie civile : Toute personne qui se prétend lésée par un crime ou un délit peut en portant plainte se constituer partie civile devant un juge d'instruction *(• art. 85 du CPP)*. Cette plainte a pour effet de déclencher une instruction par ce juge.

---

[1] *Ne sont pas concernées les actions judiciaires en responsabilité civile indépendantes d'une poursuite pénale.*
[2] *Ensemble de personnels de la police et de la gendarmerie spécialement habilités, chargés de poursuivre, rechercher et arrêter les auteurs d'infractions, sous l'autorité de l'institution judiciaire.*

CAMPUS GÉRARD MÉGIE
3, RUE MICHEL-ANGE 75794 PARIS CEDEX 16 - TÉL. 01 44 96 40 00 - TÉLÉCOPIE 01 44 96 53 90

Toutefois depuis le 1er juillet 2007, la plainte avec constitution de partie civile doit obligatoirement être précédée d'une plainte simple. Suite à cette plainte, la constitution de partie civile est recevable à condition que le plaignant justifie[3] :

- qu'un délai de trois mois s'est écoulé depuis qu'il a déposé plainte devant le procureur de la République ;
- ou que le procureur de la République lui a fait connaître, à la suite de sa plainte, qu'il n'engagera pas lui-même des poursuites (décision de classement sans suite).

I.2 – La phase d'enquête préliminaire suite à une plainte simple

La police judiciaire est chargée de constater les infractions à la loi pénale, d'en rassembler les preuves et d'en rechercher les auteurs.

Elle procède à l'enquête préliminaire (sur instruction du procureur, ou d'office). Elle constate l'infraction par procès-verbal, auditionne les personnes susceptibles d'apporter des éléments.

La police judiciaire transmet les résultats de l'enquête au procureur de la République afin qu'il prenne une décision sur la suite à donner.

Dés la découverte de l'infraction, il est indispensable :

- *de prendre toutes les précautions nécessaires sur le lieu de l'infraction avant l'arrivée des enquêteurs (ne rien déplacer, prendre des photos, ...),*
- *de faire un inventaire détaillé des biens volés ou dégradés,*
- *de faire établir dés que possible des devis pour estimer le coût de remplacement ou de réparation de ces biens,*
- *de rassembler les factures d'achats desdits biens.*
- *de collecter toute preuve utile.*

I.3 – La décision du procureur de la République

En vertu du principe de l'opportunité des poursuites, le procureur de la République peut décider :

- **d'un classement sans suite de la plainte**. Le plaignant en est informé par avis motivé.
- **de la poursuite de l'auteur de l'infraction**. L'affaire est simple (faits établis, auteur identifié) : Le procureur de la République fait convoquer l'auteur et le plaignant devant le tribunal compétent pour une audience au cours de laquelle l'affaire sera examinée et jugée.
- **d'une mesure de médiation pénale**[4] qui permet la réparation du dommage, la fin du trouble, ou le reclassement de l'auteur des faits, dans le cas d'infraction de faible gravité et sans que soit demandé au juge pénal de prononcer une sanction.
- **de l'ouverture d'une information judiciaire** et la demande de désignation d'un juge d'instruction (affaire complexe nécessitant des investigations).

---

[3] *Ces conditions de recevabilité ne sont pas requises pour les crimes et les délits prévus par la loi du 29 juillet 1881 sur la liberté de presse (diffamations, injures, offenses et outrages envers l'état, ...).*

[4] *Mesure alternative aux poursuites pénales. Sur proposition du procureur, elle réunit l'auteur et la victime d'une infraction pénale, en présence d'un tiers médiateur habilité par la justice, et consiste à trouver une solution librement négociée et à définir les modalités d'une réparation.*

Le juge d'instruction procède aux recherches, rassemble et apprécie les preuves, entend les personnes impliquées ainsi que témoins et experts, ... Il décide éventuellement de mettre en examen une ou plusieurs personnes contre lesquelles pèsent des charges sérieuses.

La police judiciaire conduit alors l'enquête sous la direction du juge d'instruction. A son terme, ce dernier prononce un non lieu s'il estime qu'il n'y a pas d'infraction ou si l'auteur n'est pas identifié clairement ou décide de renvoyer la ou les personnes mises en examen devant le tribunal compétent.

I.4 – Le jugement

C'est la nature de l'infraction qui détermine le choix de la juridiction.

- Les **contraventions**, infractions les plus légères (dégradations légères, injures, violences suivies d'une interruption temporaire de travail inférieure à 8 jours, ...) sont passibles généralement de peines d'amende prononcées par **le tribunal de police.**

- Les **délits** concernent des atteintes aux personnes, aux biens ou aux institutions (violences, homicides ou blessures involontaires, escroqueries, incendies volontaires, outrages à personnes dépositaires de l'autorité publique ou chargées d'une mission de service public, diffamation, ...). Ils sont jugés par **le tribunal correctionnel** et peuvent faire l'objet d'amendes ou de peines d'emprisonnement.

- Les infractions les plus graves, **les crimes** sont jugés par la **cour d'assises** et sont passibles de peines de réclusion criminelle.

Les tribunaux disposent également d'un éventail de peines autres que l'amende ou l'emprisonnement comme par exemple le travail d'intérêt général.

II- LES ACTEURS DU DECLENCHEMENT DE POURSUITES PENALES AU CNRS

II.1 – Qui décide d'engager une action pénale au nom du CNRS ?

Le Conseil d'Administration du CNRS délibère notamment sur :

« ... Les actions en justice et les transactions ainsi que le recours à l'arbitrage en cas de litiges nés de l'exécution de contrats de recherche passés avec des organismes étrangers »

(♦ art. 5-11° du D. n°82-993 du 24 novembre 1982 modifié portant organisation et fonctionnement du CNRS).

Le Conseil d'Administration a délégué son pouvoir au seul directeur général. Il concerne exclusivement :

« - les actions en justice contre les personnes physiques qui ne sont pas agents du CNRS ;
- l'exercice des actions pénales dirigées contre les agents du CNRS en matière d'infractions de presse et d'atteinte aux biens commises à l'encontre de l'Etablissement ;
- l'exercice des actions en justice contre les personnes morales ».

Pour l'exercice d'une partie de ces pouvoirs le directeur général a accordé une délégation de signature :

- à la directrice des affaires juridiques (DAJ)[5] ,

[5] *La DAJ a reçu délégation pour l'exercice des actions en justice dirigées contre les personnes physiques à l'exception des actions pénales introduites contres des agents du CNRS autres que celles relatives aux infractions de presse et contre les personnes morales.*

- à la directrice des ressources humaines (DRH) [6],
- au fonctionnaire sécurité défense (FSD)[7],
- aux délégués régionaux (DR)[8].

La direction des affaires juridiques est obligatoirement saisie avant tout déclenchement au nom du CNRS d'une action pénale (main courante, plainte, citation directe, ...).

En lien avec les structures et les services concernés et après examen des éléments de fait et de droit, la direction des affaires juridiques décide de l'action judiciaire la mieux adaptée à la préservation et la défense des intérêts de l'établissement.

L'instruction des actions en justice ayant trait à des atteintes aux biens (matériels et immatériels) ainsi qu'à l'image du CNRS est de la compétence exclusive de ***la direction des affaires juridiques.***

Une action pénale à l'encontre d'un agent du CNRS ne peut être menée sans l'accord préalable du Conseil d'Administration.

Aucun dépôt de plainte au nom du CNRS ne peut être introduit sans l'accord préalable de la direction des affaires juridiques.

II.2 – Comment sont engagées les poursuites pour le compte du CNRS ?

1 – La plainte ordinaire :

Si une action pénale au nom du CNRS est décidée, sa mise en œuvre par le dépôt de plainte simple peut prendre différentes voies :

■ Dépôt de plainte par un courrier adressé au procureur de la République du tribunal de grande instance du lieu de l'infraction [9] :

Ce courrier est établi et signé par le délégué régional et soumis au visa préalable de la direction des affaires juridiques.

Une copie est adressée à la direction des affaires juridiques et le cas échéant au directeur de l'unité concernée.

■ Dépôt de plainte par déposition auprès de la brigade de gendarmerie ou commissariat de police du lieu de l'infraction.

■ Dans le cas d'intrusion dans les systèmes informatiques du CNRS, en application de sa délégation de signature, le fonctionnaire sécurité défense procède au dépôt de plainte auprès des services de police spécialisés.

---

[6] *La DRH est dotée d'une délégation de signature en matière de litiges d'ordre statutaire, de pensions, d'accidents du travail et maladies professionnelles.*

[7] *Le FSD détient une délégation de signature pour le dépôt de plainte, auprès de services spécialisés, ayant trait à des intrusions dans les systèmes informatiques.*

[8] *Les Délégués ont reçu une délégation de signature pour le dépôt de plainte, après accord de la DAJ.*

[9] *Ou du domicile de l'auteur de l'infraction si il a été identifié.*

Situation d'urgence : Si les circonstances le justifient un dépôt de plainte à titre conservatoire peut être directement effectué, au nom du CNRS, par le délégué régional, qui en tient informée la direction des affaires juridiques a posteriori.

2 – La plainte avec constitution de partie civile ou la citation directe :

Ces modalités particulières, plus techniques, sont directement mises en œuvre par la direction des affaires juridiques.

III- LE SUIVI DE LA PROCEDURE PENALE AU CNRS

III.1 – Constitution du dossier d'infraction

Dés la découverte de l'infraction, le délégué régional doit adresser à la direction des affaires juridiques un dossier contenant les éléments suivants :

- la nature des faits (vol, dégradation, ...) et tous éléments de preuve constitués de photographies, constats d'huissiers, rapports, ...
- la description du dommage causé au CNRS (type de biens, existence d'assurance, le CNRS est-il propriétaire, évaluation du préjudice matériel et scientifique ...),
- un récit détaillé des circonstances (lieu, heure, avec ou sans effraction, présence de témoin, connaissance du ou des auteurs, ...).

C'est sur la base du contenu de ce dossier, que la direction des affaires juridiques apprécie, en lien avec le délégué régional et le directeur de l'unité concernés, les suites à donner.

III.2 – Suivi de la procédure

De la découverte de l'infraction au jugement, il est nécessaire, tout au long de la procédure judiciaire qui peut être longue, que le CNRS soit en mesure :

- **d'apporter toutes informations utiles aux enquêteurs :**

A titre d'exemple, les personnes ayant la qualité d'officier de police judiciaire (OPJ) peuvent sans information préalable se présenter dans les locaux du CNRS afin de procéder à une enquête sur ordre du procureur de la République (enquête préliminaire) ou d'un juge d'instruction (commission rogatoire).

Les pouvoirs d'investigation des OPJ sont étendus. Toutefois certaines opérations nécessitent l'accord du représentant du CNRS si elles n'interviennent pas dans le cadre d'une commission rogatoire (perquisitions, saisie).

- **de constituer un dossier justifiant les réclamations en dommages et intérêts et l'évaluation du préjudice [10] :**

La procédure judiciaire permet à la fois la sanction du coupable et la réparation du dommage subi. Le CNRS doit donc être en mesure de produire au juge, au plus tard au cours de l'audience, une demande en paiement de dommages et intérêts précise et justifiée.

[10] *Les dommages et intérêts alloués à une victime doivent réparer le préjudice subi sans qu'il en résulte pour elle ni perte ni profit* (Cour de Cassation 7 juin 2001).

Le montant des dommages et intérêts relève de l'appréciation souveraine du juge qui, en tout état de cause, ne pourra pas allouer une somme supérieure à celle réclamée par le CNRS. Il s'appuiera pour déterminer le montant des dommages et intérêts sur les preuves apportées.

Cette estimation est réalisée par le directeur de l'unité victime en lien avec les services de la délégation régionale.

- **d'être représenté au tribunal :**

Le CNRS est représenté à l'audience par la direction des affaires juridiques qui peut donner un mandat de représentation à un membre de la délégation régionale.

Néanmoins, dans tous les cas, des représentants de la délégation régionale et de l'unité concernés assistent à l'audience.

III. 3 – Rôle de la direction des affaires juridiques

1- Information de la direction des affaires juridiques à toutes les étapes du dossier :

La direction des affaires juridiques doit systématiquement être destinataire en copie de tous documents, communications ayant trait à l'infraction. Elle doit être tenue informée du déroulement des procédures. Cette information est primordiale pour assurer une défense réactive et cohérente des intérêts de l'établissement.

2- Choix de l'avocat :

Selon la nature du dossier l'assistance d'un avocat peut s'avérer nécessaire ou utile. La direction des affaires juridiques dispose de conseils spécialisés dans différents domaines du droit et peut les mobiliser après évaluation du besoin.

3- Préparation et soutien des acteurs impliqués dans la procédure :

En sa qualité de spécialiste des contentieux, la direction des affaires juridiques est en mesure d'éclairer les personnes impliquées dans la procédure (témoins, experts, ...) sur leur rôle et leurs obligations. Elle peut être utilement sollicitée pour la préparation ou l'assistance dans certaines opérations (audiences, recherche de preuves, ...).

DISPOSITIONS FINALES :

La circulaire n°910144SJUR du 12 avril 1991 relative aux modalités de mise en œuvre de l'intervention dans les circonstances de vol ou de dégradation commis au préjudice du CNRS est abrogée.

La présente circulaire est publiée au bulletin officiel du CNRS.

Fait à Paris, le 24 juillet 2008

Alain RESPLANDY-BERNARD
Secrétaire Général du CNRS