RÉPUBLIQUE ET CANTON DU JURA

TRIBUNAL CANTONAL

COUR ADMINISTRATIVE

ADM 92 / 2009

Président : Pierre Broglin
Juges : Sylviane Liniger Odiet, Daniel Logos, Philippe Guélat et Carmen Bossart Steulet
Greffière : Nathalie Brahier

ARRET DU 25 FEVRIER 2013

en la cause liée entre

X.
- représenté par **Me Jean-Marie Allimann**, avocat à 2800 Delémont,

recourant,

et

le Gouvernement de la République et Canton du Jura, Hôtel du Gouvernement, Rue de l'Hôpital 2, 2800 Delémont,
- représenté par **Me Marco Locatelli**, avocat à 2800 Delémont,

intimé,

relative à la décision de l'intimé du 24 juin 2009.

CONSIDÉRANT

En fait :

A.

A.1 Suite à des problèmes récurrents de saturation de la liaison Internet sur le réseau informatique de l'Etat, des analyses ont été effectuées au début du mois de novembre 2008 par le Service de l'informatique (SDI) afin de rechercher la cause de ce dysfonctionnement. Un premier contrôle de cinq jours a permis de mettre en évidence des excès dans la consultation de sites Internet non professionnels, dont des sites au contenu pornographique. Ce contrôle, effectué de manière totalement anonyme, selon le SDI, a été opéré sur l'ensemble des fichiers journaux du serveur Proxy (qui permet l'accès à Internet), et non sur des postes individuels (cf. notamment audition

du 2 mars 2010 par la CPD de A., chef du SDI, et de B., responsable du Groupe sécurité au sein du SDI, prise de position du SDI du 30 juin 2011 à la CPD).

A.2 C., averti par le SDI d'usages abusifs d'Internet, a rappelé à l'ensemble de ses collaborateurs par note interne du 20 novembre 2008 les directives du Gouvernement relatives à l'accès Internet et les consignes de D. concernant les sites dits sensibles. Il a invité toute personne ayant consulté des sites prohibés à s'annoncer auprès de lui jusqu'au 2 décembre 2008 (annexe 6 intimé). Suite aux nombreuses réactions de ses collaborateurs, C. a précisé, dans un courriel du 24 novembre 2008 adressé à l'ensemble de ses collaborateurs, que la consultation des sites érotiques était interdite. Il indiquait en outre qu'aucune sanction n'était prévue mais qu'un simple rappel à l'ordre serait adressé à celles et ceux qui auraient consulté des sites interdits ne tombant pas sous le coup du Code pénal (annexe 7 intimé).

A.3 Compte tenu des moyens techniques limités du SDI à l'époque et de l'impossibilité d'identifier les personnes concernées, le SDI a mandaté une société externe, SCRT à Préverenges, pour effectuer l'analyse des fichiers journaux (logs) du Proxy permettant l'accès à Internet depuis le réseau interne du canton. Cette analyse a porté sur tous les postes de l'administration. Cette société a dès lors effectué une analyse globale anonyme sur l'ensemble du trafic Internet via le serveur Proxy du canton pour le mois de novembre 2008. La société SCRT a confirmé, dans son rapport du 19 décembre 2008, que certains collaborateurs accédaient à des sites Internet sans rapport avec leur activité professionnelle, respectivement à des sites à caractère pornographique. Les sites visités, ainsi que leurs périodes de fréquentations, des machines ayant effectué le plus grand nombre de hits (appel vers une donnée présente sur un serveur web, étant précisé qu'une page compte entre dix et vingt données) ont été analysés et retranscrits dans ce rapport (cf. CD figurant dans le dossier Cour adm. p. 136).

A.4 Sur cette base, le SDI a pu faire l'association entre la machine et l'utilisateur pour un certain nombre de cas. Ces résultats ne pouvaient toutefois être utilisés sans vérification supplémentaire, compte tenu de paramètres incontrôlables et de la possibilité que plusieurs utilisateurs partagent la même machine. Dans une seconde phase, SCRT a repris les résultats de la première phase et a contrôlé, sur les postes de travail, quels utilisateurs avaient des historiques Internet Explorer contenant des accès à des sites problématiques. Pour ce faire, le SDI a pris contact téléphoniquement avec les 56 utilisateurs concernés, leur a demandé l'autorisation de prendre leur ordinateur en télémaintenance, sans pour autant expliquer la nature exacte de cette opération et sa finalité. Un employé de SCRT lançait alors un programme permettant de récupérer les informations et les sauvegardait pour analyse (cf. notamment audition du 2 mars 2010 par la CPD de A. et de B. et prise de position du SDI du 30 juin 2011 à la CPD).

B. Le 11 février 2009, le SDI a transmis le dossier au Gouvernement qui en a pris connaissance le 17 février 2009 et a ordonné l'ouverture d'enquêtes disciplinaires en date des 27 février et 3 mars 2009 à l'encontre de 28 personnes (cf. rapport final de

la commission d'enquête disciplinaire du 15 mai 2009 figurant au dossier de la CPD). Une enquête disciplinaire a notamment été ouverte à l'encontre de X. (ci-après : le recourant), (…). Dans le cadre de cette enquête, le disque dur de son ordinateur a été saisi et les données de ce dernier ont été copiées (cf. rapport final précité et p. 1.1ss du dossier PER – Enquête disciplinaire N 17).

C.

C.1 Dans son rapport principal intitulé "Rapport d'analyse forensique" effectué après la saisie du disque dur du recourant, le 26 mars 2009 (cf. annexe 1 intimé, p. 3 et 4), SCRT reprend tout d'abord l'analyse des "hits" du 1er au 30 novembre 2008 de la machine ayant l'adresse IP 10.28.61.40, analyse figurant dans son rapport du 19 décembre 2008 au chiffre 3.18 (cf. CD figurant dans le dossier Cour adm. p. 136). Il en ressort que son utilisateur a consulté des sites pornographiques de la façon suivante :

10.11.2008	17h00	154 hits
12.11.2008	17h00	1 hit
17.11.2008	17h00	232 hits
18.11.2008	12h00	122 hits
	18h00	11 hits
19.11.2008	18h00	413 hits
	19h00	152 hits
27.11.2008	18h00	2 hits

C.2 Dans ce même rapport principal, SCRT indique ensuite que l'analyse du disque dur de l'ordinateur utilisé par le recourant a permis de confirmer dans un premier temps que cette machine a été utilisée pour consulter des sites web à caractère pornographique, soit 1788 images de juillet 2008 à mars 2009 et 143 vidéos d'août 2008 à mars 2009 (annexe 1 intimé, p. 10 et 12). Dans un rapport complémentaire du 11 mai 2009 intitulé "Complément au Rapport d'analyse forensique" faisant suite à une seconde analyse portant uniquement sur l'utilisation par le recourant lui-même de son ordinateur, SCRT indique que ces résultats se réduisent à 264 images à caractère pornographique téléchargées du 24 juillet au 6 août 2008 et le 1er mars 2009, ainsi qu'au téléchargement de 28 vidéos du 31 juillet au 6 août 2008 et le 1er mars 2009 (annexe 5 intimé, p. 5 à 7).

C.3 Interpellé par la commission d'enquête (cf. p. 7 du dossier PER – Enquête disciplinaire N 17), C. (…), a indiqué que le recourant donne satisfaction dans l'exécution de son travail et s'investit dans sa mission conformément aux attentes. Il privilégie l'action à la réflexion, sans toutefois que cela ne porte préjudice à son activité. Le recourant n'a pas annoncé la consultation de sites Internet pour adultes (suite à sa note du 20 novembre 2008, cf. consid. A.2 ci-dessus).

C.4 Le recourant a été entendu le 27 mars 2009 par la commission d'enquête (cf. p. 8.1ss du dossier PER – Enquête disciplinaire N 17). Il a déclaré travailler sur un ordinateur portable qui doit rester à disposition de ses collègues ; il arrive toutefois rarement qu'il

soit utilisé par d'autres personnes que lui-même. Son ordinateur restait en permanence allumé jusqu'en mars 2009, de sorte qu'il n'avait pas besoin d'introduire son identifiant pour se connecter. Le recourant admet avoir consulté des sites à caractère pornographique, mais uniquement en dehors de ses heures de bureau. Il visitait de tels sites quelques fois par semaine, à raison d'une heure ou deux par connexion, afin de se détendre en fin de journée. Le recourant n'a jamais eu l'impression de faire quelque chose de répréhensible, soit notamment de ralentir le réseau informatique cantonal. Il effaçait régulièrement l'historique des sites consultés, afin que le prochain utilisateur ne voie pas les sites qu'il avait consultés.

C.5 Dans son rapport du 16 avril 2009 (p. 9.1ss du dossier PER – Enquête disciplinaire N 17), la commission d'enquête disciplinaire relève que le recourant a fait usage de connexions Internet à réitérées reprises, à raison d'une à deux heures par connexion et ce plusieurs fois par semaine, dans un but totalement étranger à son activité professionnelle durant plusieurs mois. En consultant des sites à caractère pornographique, le recourant a enfreint ses devoirs de fonction. Il devait avoir conscience que son comportement était propre à porter atteinte à l'image de la RCJU et était susceptible de contribuer à la saturation du réseau. Les directives en la matière sont claires et le recourant devait en avoir eu connaissance. Son comportement est d'autant moins excusable ensuite de l'avertissement formel de C. Compte tenu de ces éléments, la commission d'enquête considère la faute du recourant de moyenne à grave. Toutefois, au vu de la durée de ses rapports de service, de l'absence d'antécédents, du bon rapport de C., du fait que les agissements du recourant ont eu lieu en bonne partie en dehors des heures de travail et de la bonne collaboration du recourant, sa faute doit être qualifiée de moyenne.

Dans son complément du 15 mai 2009 (p. 19.1ss du dossier PER – Enquête disciplinaire N 17), après avoir respecté le droit d'être entendu du recourant, la commission d'enquête précise que son rapport ne se base pas sur des dates de consultations déterminées, mais bien plutôt sur les déclarations du recourant qui admet avoir consulté des sites à caractère pornographique plusieurs fois par semaine à raison d'une à deux heures par connexion. La commission retient également, faute de preuve, que ces consultations ont eu lieu pour la plupart en dehors des heures de travail. En permettant à un tiers de se loguer sur son poste, le recourant a par ailleurs violé le principe de confidentialité dans le traitement de son identifiant. En outre, le fait de consulter des sites pornographiques, même en dehors des heures de travail est propre à porter atteinte à l'image de la RCJU.

C.6 Au vu des rapports susmentionnés, le Gouvernement a, par décision du 24 juin 2009, transféré le recourant dans une classe inférieure de traitement soit de la classe 12 à la classe 11 avec effet au 1er août 2009 et cela pour une période de cinq ans et mis à sa charge les frais par CHF 1'000.- (PJ 2 recourant).

D.

D.1 X. a interjeté recours contre la décision précitée le 15 juillet 2009. Il conclut à l'annulation de cette dernière, à ce qu'il ne soit pas prononcé de sanction disciplinaire

à son encontre, subsidiairement, à ce qu'il soit prononcé un blâme, très subsidiairement, à ce que ce blâme soit assorti d'une amende de CHF 150.-, sous suite des frais et dépens.

Le recourant fait valoir en substance que son transfert dans une classe inférieure durant cinq ans représente un préjudice supérieur à CHF 20'000.-. Il admet avoir consulté des sites à caractère pornographique, mais uniquement en dehors de ses heures de travail. Il ne considère dès lors pas avoir adopté un comportement punissable. Il ne se trouvait par ailleurs pas sur son lieu de travail à certaines dates qui ressortent du rapport, soit notamment les 24, 27, 30, 31 juillet et 1er août 2008, ainsi que les 3, 4, 15 et 16 janvier 2009, de sorte que ce n'est pas lui qui a consulté des sites Internet aux dates indiquées. Le fait que des tiers aient utilisé son ordinateur et son login ne saurait lui être imputé. L'échange de postes informatiques et de login était usuel à cette époque (…). Il laissait fréquemment son poste allumé afin que ses collègues puissent en disposer rapidement, (…). Le recourant se prévaut ensuite d'une violation du principe de l'égalité de traitement. Dans la mesure où il n'a pas consulté de sites pénalement répréhensibles et qu'il a consulté des sites à caractère érotique uniquement en dehors de son temps de travail, le recourant estime que son comportement ne saurait être plus sévèrement puni que celui des employés qui consultent des sites tels que Facebook, la Redoute etc. durant leur temps de travail ou de ceux qui s'absentent régulièrement pour fumer une cigarette. Le principe de la proportionnalité a également été violé, la sanction prononcée à son encontre étant disproportionnée ; il n'a commis tout au plus qu'une faute légère. Il invoque également une violation du principe de la bonne foi, C. ayant annoncé dans sa note du 24 novembre 2008 qu'aucune sanction ne serait prononcée.

D.2 Dans sa réponse du 29 septembre 2009, le Gouvernement conclut au rejet du recours, dans la mesure où il est recevable, sous suite des frais et dépens. Il relève à l'appui de ses conclusions que le recourant a consulté des sites à caractère pornographique durant son temps de travail en précisant que l'analyse n'a pas permis de retrouver la trace de toutes les consultations du recourant, une partie des données pouvant automatiquement être "écrasée" par le système. Toutefois, l'analyse effectuée démontre que le recourant a consulté des sites pornographiques les 10, 12 et 17 novembre 2008 durant son temps de travail, étant précisé que son horaire se termine à 18h00. Plusieurs images et vidéos ont été visionnées en janvier et février 2009. Le fait que le recourant ait effacé son historique et continué son activité malgré la note de D. du 30 août 2008 puis de C. du 20 novembre 2008 et du courriel de ce dernier du 24 novembre 2008 démontre qu'il avait parfaitement conscience du caractère répréhensible de son comportement. Le fait que le recourant n'ait pas sécurisé son ordinateur et sa session constitue également une faute de comportement. La consultation de sites pornographiques durant ou en dehors du temps de travail est de nature à porter atteinte aux intérêts de l'Etat, notamment à sa réputation. Il suffit de voir les retombées médiatiques de cette affaire pour s'en convaincre. Le comportement du recourant, compte tenu de la fréquence de ses consultations et du genre de celles-ci, ne saurait être comparé à celui de fonctionnaires consultant des sites tels que la Redoute, RFJ, etc. En outre, le

recourant a poursuivi ses agissements en janvier et février 2009, malgré la mise en garde de C., dénotant ainsi un mépris flagrant des consignes. La sanction prononcée est proportionnée à son comportement au vu de la durée et de la fréquence de ses agissements, de la poursuite de ceux-ci après l'avertissement de C. et de sa fonction. Dans la mesure où le recourant ne s'est pas annoncé auprès de C. suite à son message, il ne saurait se prévaloir du principe de la bonne foi.

D.3 Une audience s'est tenue le 17 mars 2010 devant la Cour de céans (dossier Cour adm. p. 58ss).

D.3.1 Lors de son interpellation, le recourant a répété avoir consulté des sites de pornographie conventionnelle uniquement en dehors de son temps de travail. Il n'a jamais eu l'impression de violer une règle, y compris après le message de C. qui se référait à l'article 197 CP, disposition qu'il n'a pas enfreinte. Le service (…) qui est mentionné dans le plan de service est également appelé service libre. Il permet aux *employés de travailler* sans la pression d'un service de piquet. Durant ce service, le nombre d'heures de travail doit être effectué, soit huit heures, mais les *employés* peuvent aménager leur horaire. Il se pouvait dès lors que le recourant débute sa journée à 06h00 et qu'il la termine à 17h00. La différence avec le service (…) ou (…) est que dans ces situations, les *employés* sont susceptibles d'être appelés à tout moment durant le service de piquet. Ce plan de service correspond à la réalité, il n'y a pas eu de changements. Avant janvier 2009, les heures d'arrivée et de départ n'étaient pas notées. De façon générale, le recourant efface son historique et ce également lorsqu'il consulte des sites professionnels. Il laissait son ordinateur allumé en son absence pour des questions d'efficacité. Le programme (…) et le programme (…) étaient installés sur son poste et son service bénéficie de très peu de licences. Il lui arrive pour sa part d'utiliser l'ordinateur de ses collègues, notamment pour effectuer (…).

D.3.2 E., entendue au nom de l'intimé, a indiqué que toutes les personnes qui se sont annoncées suite au courriel de C. ont fait l'objet d'une procédure disciplinaire. Un cas n'a pas fait l'objet de sanction, car il ne s'agissait en fait pas d'images pornographiques.

D.3.3 C. a précisé que jusqu'au 31 décembre 2008 il n'y avait pas de surveillance stricte du temps de travail ; les *employés* travaillaient au forfait. Le recourant pouvait effectivement terminer sa journée à 17h00 s'il avait effectué ses heures. Il n'y avait pas de moyens de contrôle, cela fonctionnait selon le principe de la confiance. C. a été informé par le SDI de l'usage abusif d'Internet le 6 novembre 2008. Il n'était pas encore question d'enquêtes à cette période. Six enquêtes disciplinaires concernaient des membres *de son service*. Une enquête a abouti à un avertissement, il s'agissait d'une personne qui donnait son login et a été sanctionnée pour ce fait.

D.3.4 F., (…), a confirmé qu'il est possible de terminer sa journée à 17h00 dans le cadre d'un service (…), si le nombre d'heures a été effectué. Il est vrai que les ordinateurs restent souvent allumés et ce encore aujourd'hui, notamment lorsqu'il faut agir en

urgence. Plusieurs programmes requièrent des licences. Il y a par exemple deux licences pour le programme (…), mais plusieurs postes sont équipés de ce programme. Le programme n'est pas lié à la session, mais est sur l'ordinateur. Il faut introduire le mot de passe pour y accéder. F. et le recourant disposent d'un mot de passe, lesquels sont accessibles à tout le monde. L'ordinateur peut donc être éteint sans problème et ne doit pas rester allumé.

D.3.5 B. a également été entendu et s'est exprimé sur la procédure suivie par le SDI et la société SCRT. Il a notamment indiqué qu'il y avait eu une collecte d'informations du 1er au 5 novembre 2008 sur l'ancien système Proxy. Il n'y avait toutefois pas à cette époque de possibilité d'identifier l'ordinateur et le numéro d'inventaire, de sorte qu'il a fallu procéder autrement. Dans l'absolu, il aurait fallu saisir tous les disques durs dans tous les services identifiés. L'analyse effectuée du 1er au 5 novembre a permis d'identifier certains problèmes, notamment au niveau *du service du recourant*. La société SCRT a alors été mandatée pour faire une analyse plus large sur tout le mois de novembre. Comme la liste fournie par SCRT était assez large, il a fallu l'affiner. Un mandat a alors été donné à SCRT qui a agi par le biais d'un logiciel. Comme celui-ci devait être exécuté sur l'ordinateur susceptible d'être problématique, le SDI devait obtenir la prise en main mais il fallait l'accord de l'utilisateur. A cet effet, on a invoqué un problème d'accès à Internet. Il était ainsi possible d'associer un numéro d'inventaire à des traces d'accès à des sites. La société opérait depuis les locaux du SDI. Ce processus a été fait pour éviter de saisir trop de disques durs.

D.3.6

D.3.6.1 G., directeur de la société SCRT, a précisé, lui, que sa société n'a pas été impliquée dans la procédure et les démarches. Elle n'a notamment pas initié la démarche de prise en main des postes des utilisateurs concernés. Cette démarche était toutefois utile et il aurait été impossible techniquement de saisir tous les disques durs et de les analyser. Cette manière de faire a permis de vérifier si les adresses IP identifiées au départ étaient toujours les mêmes, étant précisé qu'une adresse IP peut changer. Interpellé quant à la différence entre le rapport principal et le rapport complémentaire, G. a indiqué que le rapport complémentaire a permis de cibler plus précisément les images et vidéos contenues uniquement dans le cache du navigateur de l'utilisateur (…), soit celui du recourant. Le premier rapport portait sur l'analyse de l'adresse IP. C'est le rapport complémentaire qui est déterminant.

D.3.6.2 A la demande de la Cour de céans, G. a précisé dans un rapport du 8 juin 2010 (dossier Cour adm. p. 111ss) que le rapport complémentaire du 11 mai 2009 avait permis de cibler les images contenues uniquement dans le cache du navigateur de l'utilisateur (…). Le premier rapport du 26 mars 2009 fait état des images et vidéos retrouvées sur la machine, alors que le rapport complémentaire fait état des images et vidéos retrouvées sur la machine et qui ont pu être attribuées avec certitude à l'utilisateur (…) (soit le recourant). Sans avoir accès aux machines concernées, que ce soit par la prise en main à distance ou par la saisie des disques durs, il était impossible de s'assurer du nom de l'utilisateur ayant consulté des sites non professionnels. L'adresse IP était susceptible de changer et en outre certaines

machines étaient utilisées par plusieurs personnes. G. a en outre récapitulé les hits pouvant être attribués avec certitude à l'utilisateur (…).

D.3.6.3 En réponse à des questions complémentaires posées par la Cour de céans, G. a précisé le 23 juillet 2010 (dossier, p. 132ss), qu'il aurait été difficile de saisir et d'analyser les 54 disques durs en cause, notamment en raison du temps et des coûts d'une telle procédure, étant précisé que chaque disque à analyser nécessite plusieurs jours de travail. Le risque de saisir de mauvaises machines et l'effet traumatisant qui en aurait résulté préconisaient également de prendre en main à distance les postes des utilisateurs concernés.

E.

E.1 Parallèlement à son recours, le recourant a saisi la Commission de protection des données (CPD) le 16 mars 2010 afin de faire constater le caractère illicite du moyen de preuve utilisé ayant conduit à une sanction disciplinaire à son encontre. Il a sollicité la suspension de la présente procédure jusqu'à droit connu dans celle introduite devant la CPD. Il a été fait droit à cette requête par décision du 16 août 2010.

E.2 La CPD a procédé à différentes mesures d'instruction, dont notamment l'audition de A. et B. (cf. procès-verbal de la séance du 2 mars 2010). Il en ressort notamment que la surveillance effectuée en novembre 2008 et le rapport du 19 décembre 2008 de la société SCRT ne permettaient pas d'identifier précisément les utilisateurs concernés, compte tenu du fait qu'une adresse IP peut varier d'un jour à l'autre. Il était nécessaire de procéder à des contrôles supplémentaires. La prise en main à distance avait pour objectif de réduire le nombre de postes de travail à traiter par la suite et d'éliminer tout faux positif. Cette étape a ainsi permis de passer de 54 à 30 postes, d'arriver devant le Gouvernement avec un dossier solide et d'éviter de saisir trop de disques durs. Les rapports du SDI, puis ceux élaborés par SCRT durant cette étape, n'ont pas été utilisés ni versés aux dossiers des procédures disciplinaires ; ces données sont conservées au SDI.

E.3 Dans sa décision du 29 mars 2012, la CPD constate dans un premier temps que les informations mises en rapport avec les adresses IP des postes informatiques doivent être tenues pour des données personnelles (consid. 2.1.1 i.f.). Quant aux données relatives aux communications, tels que les fichiers journaux (log files) permettant de déterminer quand et depuis quel ordinateur une page Web a été consultée, elles sont généralement considérées comme sensibles. Compte tenu des circonstances du cas, la CPD a dès lors admis que les données collectées par le SDI pendant le mois de novembre doivent être considérées comme sensibles (consid. 2.1.2). Dès lors, la directive de l'intimé du 13 mars 2001 relative aux enregistrements et à la surveillance informatique ne représente pas une base légale formelle suffisante permettant au SDI de traiter des données personnelles sensibles au sens de l'article 5 al. 2 litt a LPD. La CPD indique par conséquent que c'est uniquement dans le cadre d'une procédure d'enquête disciplinaire, au sens de l'article 32 aLStMF, que l'analyse et l'utilisation des fichiers journaux pouvaient être réalisées en respectant le principe de la légalité (consid. 2.2.1). Or, en l'espèce, un certain nombre d'analyses ont été effectuées avant

l'ouverture d'enquêtes disciplinaires et sans instruction des autorités compétentes (Gouvernement ou Conseil de surveillance de la magistrature) pour ouvrir de telles enquêtes. Il s'agit en particulier de la surveillance effectuée durant le mois de novembre 2008. Celle-ci constitue un traitement de données illicite, dès lors que le SDI n'était pas en mesure de se prévaloir d'une tâche légale qui l'aurait autorisé à analyser les fichiers journaux en vue d'identifier les auteurs des connexions à des sites problématiques ou simplement les postes de travail de ceux-ci ou de réunir les preuves de telles connexions (consid. 2.2.1-2.2.5). La prise en main à distance des postes informatiques réalisée par la suite sans préciser la nature exacte de l'opération à l'utilisateur contrevient au principe de la bonne foi et était également illicite au sens de la loi jurassienne sur la protection des données (consid. 3). La CPD a finalement considéré que, quand bien même les données collectées par le SDI au moyen des analyses de fichiers journaux, fin 2008 et début 2009, l'ont été de manière illicite, les mêmes données auraient pu valablement, au sens de la LPD, être réunies par l'autorité disciplinaire elle-même, de sorte que cette dernière était en droit de les utiliser a posteriori dans le cadre des enquêtes disciplinaires. Il en va de même des données collectées par l'autorité disciplinaire elle-même au moyen de la saisie et de l'analyse des disques durs (consid. 4.1). La CPD a refusé dès lors d'ordonner la destruction de ces données pour ce motif. En revanche, les données obtenues au moyen de la prise en main à distance, qui n'ont pas été versées dans les dossiers disciplinaires, doivent être détruites (consid. 4.2). La CPD a toutefois relevé que la Cour administrative n'était pas liée par sa décision admettant le principe de l'utilisation par l'autorité disciplinaire de preuves obtenues illicitement par le SDI (consid. 4.3).

F.

F.1 Dans ses remarques finales du 13 août 2012, le recourant relève en substance que l'administration de la preuve a permis d'établir qu'il n'avait consulté des sites à caractère pornographique qu'en dehors de son temps de travail. En son absence, son poste restait allumé pour des raisons de sécurité et de confiance. S'agissant plus particulièrement de la décision de la CPD du 29 mars 2012, le recourant conteste sa motivation selon laquelle les données collectées illicitement auraient pu l'être de manière légale et seraient donc susceptibles d'être utilisées dans le cadre de la présente procédure disciplinaire. Selon le recourant, les fichiers électroniques en cause ne peuvent être utilisés comme moyens de preuve selon l'article 59 al. 2 Cpa. Faute de preuves, on ne saurait considérer qu'il n'a pas agi loyalement dans le cadre de ses rapports de travail. En tous les cas, dans la mesure où la sanction prononcée à son encontre tend à réprimer un comportement fautif et à empêcher la récidive, il y a lieu d'appliquer l'article 6 CEDH. Or, en application de cette disposition et dans la mesure où il n'a pas commis d'infraction grave, les moyens de preuve obtenus illicitement ne sauraient être utilisés.

F.2 De son côté, l'intimé a indiqué qu'il n'avait pas de remarques complémentaires à faire valoir.

F.3 Il sera revenu ci-après, en tant que besoin, sur les autres éléments du dossier.

<u>En droit</u> :

1.

1.1 La décision attaquée est fondée sur la loi sur le statut des magistrats, fonctionnaires et employés de la République et Canton du Jura (LStMF ; RSJU 173.11), abrogée par l'actuelle loi sur le personnel de l'Etat (LPer ; RSJU 173.11), entrée en vigueur le 1er janvier 2011.

Selon l'article 98 LPer, les procédures pendantes au moment de l'entrée en vigueur de la loi, notamment les résiliations, les enquêtes disciplinaires et les suspensions, restent soumises à l'ancien droit. Il ne peut plus être prononcé de sanctions disciplinaires dès l'entrée en vigueur de la loi.

En l'espèce, le transfert du recourant dans une classe inférieure de traitement au sens de l'article 31 al. 1 let. d LStMF constitue une sanction disciplinaire prononcée à l'issue de la procédure disciplinaire.

C'est dès lors la LStMF qui s'applique en l'espèce, cette sanction ayant été prononcée le 24 juin 2009, soit avant l'entrée en vigueur de la LPer.

1.2 Il découle de l'article 51 let. a LStMF que la procédure et la compétence sont fixées par le Cpa s'agissant du recours du fonctionnaire envers l'Etat contre une décision touchant ses rapports de service et sa situation. La Cour administrative est compétente pour connaître des recours formés contre les décisions prises par le Gouvernement (art. 160 let. a Cpa).

La compétence de la Cour administrative, statuant dans une composition à cinq juges (cf. art. 24 al. 2 let. a LOJ), est ainsi donnée.

1.3 Pour le surplus, interjeté dans les formes et délai légaux par une personne disposant manifestement de la qualité recourir, le recours est recevable, de sorte qu'il y a lieu d'entrer en matière.

2. Sur recours de droit administratif contre une sanction disciplinaire plus sévère que le blâme, l'amende jusqu'à 200 francs ou la suspension jusqu'à cinq jours, le pouvoir d'examen de la Cour administrative porte sur la violation du droit, y compris l'excès ou l'abus du pouvoir d'appréciation, la constatation inexacte ou incomplète des faits pertinents, ainsi que sur l'inopportunité de la décision attaquée (art. 122 let. a, b et c ch. 2 Cpa).

3.

3.1 Aux termes de l'article 30 al. 1 LStMF, le fonctionnaire qui enfreint ses devoirs de service, intentionnellement ou par négligence, est passible d'une sanction disciplinaire. Il découle en outre de l'article 20 al. 1 LStMF que le fonctionnaire doit agir conformément à la loi et aux intérêts de l'Etat. L'article 21 al. 1 LStMF lui impose de se montrer digne de la considération et de la confiance qu'exige sa fonction

publique, par son comportement général en et hors service. Ces deux dispositions, en vigueur jusqu'au 31 décembre 2010, s'imposaient à l'évidence au recourant lorsqu'il était encore en service. La teneur de l'article 20 al. 1 LStMF a d'ailleurs été reprise à l'article 21 al. 2 LPer.

3.2 Les directives concernant les modalités d'utilisation d'Internet et de la messagerie au sein de l'Administration cantonale du 13 mars 2001 prévoient notamment sous le point 1, Introduction, que les postes de travail et autres systèmes de traitement de l'information ne peuvent être utilisés que dans le cadre des activités du Service. Une utilisation à but privé doit rester exceptionnelle durant le temps de travail. Elle est autorisée en dehors des heures de travail. Au point 3.2, chiffre 1, il est précisé que le collaborateur ne doit pas télécharger, posséder, diffuser ou afficher des documents ou fichiers ayant des contenus illicites. De même, il ne doit pas adopter des comportements dangereux pour la sécurité des données, ou portant atteinte aux intérêts et à l'image de la RCJU ou de personnes.

4.

4.1 Pour rendre sa décision, l'intimé s'est fondé sur le rapport de la Commission d'enquête, laquelle s'est elle-même basée sur les mesures d'investigations réalisées par le SDI, respectivement la société SCRT dès novembre 2008, ainsi que sur les analyses du disque dur saisi en mars 2009 et les déclarations du recourant. Ce dernier conteste la licéité des moyens de preuves précités.

4.2 La surveillance de novembre 2008 a porté sur l'analyse des "fichiers journaux" (log files). Ces derniers indiquent notamment quand et depuis quel ordinateur une page Web a été consultée. Les données relatives aux communications mais aussi celles relatives au contenu de ces dernières peuvent faire l'objet d'une analyse se rapportant aux personnes. Or, certaines de ces données personnelles sont sensibles et leur analyse peut permettre de constituer des profils de la personnalité (cf. message du CF concernant la modification de la loi sur l'organisation du gouvernement et de l'administration, FF 2009 p. 7695). Les choix de navigation sont susceptibles de porter sur des traits essentiels de la personnalité et du comportement du travailleur (MEIER, Protection des données, Fondements, principes généraux et droit privé, Berne 2011, n. 2207). Il s'ensuit que la récolte de "fichiers journaux" constitue sans aucun doute une atteinte à la sphère privée, de telle sorte qu'une base légale est nécessaire pour y procéder.

4.3 La question de savoir quels sont les moyens de preuve admis et comment le juge établit les faits pertinents pour prononcer les mesures administratives adéquates relève de la procédure administrative, régie en principe par le droit cantonal. Dans le canton du Jura, les autorités constatent les faits d'office (art. 58 Cpa). L'autorité procède aux investigations nécessaires, en recourant s'il y a lieu aux moyens de preuve énumérés à l'article 59 al. 1 Cpa, tels que : titres, rapports, livres et autres documents officiels et privés (cf. let. a). D'autres moyens de preuve que ceux énumérés à l'article 59 al. 1 Cpa peuvent être utilisés s'ils sont propres à fournir la preuve et s'il n'en résulte pas une atteinte à la liberté personnelle. Tel est par exemple

le cas d'enregistrement de sons ou d'images (art. 59 al. 2 Cpa ; BROGLIN, Manuel de procédure administrative jurassienne, Courrendlin 2009, n. 176). Cet alinéa confirme le principe selon lequel une base légale est nécessaire pour tout moyen de preuve qui imposerait au justiciable un comportement ou restreindrait sa sphère privée (MOOR / POLTIER, Droit administratif, vol. II, Berne 2011, p. 297 ; BOVAY, Procédure administrative, Berne, 2000, p. 188).

4.4 Le terme "document" figurant à la lettre a de l'article 59 al. 1 Cpa doit être interprété au regard de l'évolution des progrès techniques et permet de prendre en compte les nouveaux moyens (BOVAY, op. cit., p. 188). Dans ce sens, il convient d'admettre que ce terme comprend les fichiers électroniques, respectivement les fichiers journaux. L'article 177 CPC, applicable pour le surplus par renvoi de l'article 69 Cpa, prévoit du reste expressément que les fichiers électroniques sont des titres. Par ailleurs, au plan fédéral, les fichiers électroniques sont considérés par la jurisprudence comme une preuve documentaire au sens de l'article 12 PA, dont le contenu est similaire à celui de l'article 59 al. 1 Cpa (JAAC 68.1 consid. 6 et les références citées). Il s'ensuit que l'article 59 al. 1 let. a Cpa ne saurait être interprété aussi restrictivement que le souhaite le recourant. Il convient dès lors d'admettre que l'article 59 al. 1 Cpa constitue une base légale suffisante pour utiliser en tant que moyens de preuve des fichiers électroniques, respectivement des fichiers journaux d'accès Internet, ces derniers étant compris dans la notion de documents.

4.5 Au vu de l'atteinte à la liberté personnelle, respectivement au respect de la sphère privée découlant de l'analyse de "fichiers journaux", le respect du principe de la proportionnalité ainsi qu'un intérêt public prépondérant sont nécessaires en plus de la nécessité d'une base légale suffisante, pour admettre une restriction à ce droit fondamental (cf. ATF 130 I 65 consid. 3.3). L'intérêt public de l'administration au respect de ses directives en matière d'utilisation d'Internet, à une correcte exécution du travail de ses employés ou à son image justifie sans aucun doute la mise en place de contrôles de fichiers journaux, respectivement une atteinte à la liberté personnelle de ses employés. Concernant le respect du principe de la proportionnalité, la Cour de céans renvoie aux considérants de la décision de la CPD sur ce point (cf. consid. 2.2.1) qu'elle fait siens. Il s'ensuit qu'un contrôle anonymisé ou pseudonymisé puis, en cas de soupçon concret, un contrôle nominatif des fichiers journaux, tels que prévus par les directives, permettaient de respecter ce principe.

5.

5.1 Les sanctions disciplinaires sont prononcées par le Gouvernement (art. 33 al. 1 LStMF). Sous réserve d'une délégation à l'un de ses membres, à un service subordonné, à un fonctionnaire, voire à des personnes extérieures à l'administration, le Gouvernement instruit lui-même l'affaire (art. 50 al. 1 à 3 Cpa).

5.2 En l'espèce, l'analyse des fichiers journaux a été effectuée par le SDI, respectivement la société SCRT sur mandat du SDI.

Dans un article intitulé "Les enseignements à tirer de la surveillance illicite de magistrats et fonctionnaires par un service informatique - Commentaire de l'affaire jurassienne du Pornogate" (Jusletter du 3 septembre 2012), Sylvain Métille relève que le SDI devait chercher à identifier les problèmes d'accès en se contentant au maximum de détecter les problèmes de volume de trafic et en bloquant les sites posant problèmes. S'il avait des doutes sur la commission d'infractions pénales ou de comportements susceptibles d'être sanctionnés administrativement, il devait en référer à l'autorité compétente. Il pouvait éventuellement suggérer des démarches techniques ou proposer son assistance. En aucun cas en revanche, il ne devait prendre l'initiative de conduire des mesures de surveillance (n. 25). Pour atteindre le but initial, à savoir déterminer la cause des lenteurs et des dysfonctionnements dans l'accès à Internet constatés lors de la diffusion de la session du Parlement jurassien à l'automne 2008, des mesures moins attentatoires à la sphère privée étaient envisageables : un blocage de l'accès à certains sites considérés comme problématiques ou une simple limitation du débit de téléchargement depuis les sites trop gourmands en bande passante aurait suffi à résoudre le problème. Un tel blocage aurait respecté l'exigence de proportionnalité et pouvait être mis en place sans grande difficulté. D'une démarche initiale visant à localiser la source d'un gros volume de données, indépendamment de leur contenu, le SDI s'est retrouvé dans un rôle d'enquêteur cherchant à prouver la commission d'infractions pénales (n. 1, 11 et 12). La Cour de céans partage ce point de vue, à tout le moins s'agissant des actes accomplis par le SDI après le premier contrôle de cinq jours, effectué du 1er au 5 novembre 2008, qui avait permis de mettre en évidence des excès dans la consultation de sites Internet non professionnels, dont des sites au contenu pornographique. Il suit de là que l'extension de la surveillance au-delà du 5 novembre par le SDI était illicite de même que les analyses effectuées par SCRT après ce premier contrôle de cinq jours, dès lors qu'elles ont été ordonnées par le SDI qui n'était pas légitimé à le faire et qui, pour l'exercice de ses tâches, à savoir détecter la cause des lenteurs et des dysfonctionnements dans l'accès à Internet, pouvait parfaitement agir d'une autre manière pour respecter le principe de proportionnalité.

La saisie du disque dur et l'interpellation du recourant ont en revanche été effectuées par la Commission d'enquête désignée par le Gouvernement (cf. décision du Gouvernement du 3 mars 2009, p. 1.1 du dossier PER – Enquête disciplinaire N 17). Il apparaît dès lors que seule la saisie du disque dur et les déclarations du recourant ont été recueillies de manière légale, à savoir à la suite d'une décision de l'autorité disciplinaire compétente. Le SDI n'était au bénéfice d'aucune délégation de compétence lui permettant de procéder lui-même ou de faire procéder à l'analyse des fichiers journaux, comme on vient de le voir. Il est renvoyé pour le surplus à la décision de la CPD (cf. consid. 2.2.3). L'analyse effectuée par SCRT portant sur la période de novembre 2008 doit dès lors être considérée comme illicite.

Il sera revenu, ci-après, sur le sort des preuves secondaires, soit de la saisie du disque dur et des déclarations du recourant (cf. consid. 6.3.3).

5.3 Il y a en premier lieu d'examiner si la preuve originaire, soit l'analyse effectuée par SCRT, considérée comme illicite, peut être exploitable.

6.

6.1 En procédure administrative, le sort de preuves obtenues de manière illicite n'est réglé ni dans la loi jurassienne, ni dans la loi fédérale. En procédure pénale, il est admis que l'utilisation d'une preuve obtenue de manière illicite ne peut être prise en considération que si l'autorité eût pu en avoir connaissance régulièrement ou si un intérêt public important le justifie. Ce principe jurisprudentiel a certes été posé en matière pénale où l'ordre public commande impérativement que la lumière soit faite par tous les moyens possibles, mais la doctrine majoritaire et le Tribunal fédéral admettent qu'il vaut aussi en procédure administrative (MOOR / POLTIER, op. cit., p. 297 ; BROGLIN, op. cit. n. 175, AUER / MALINVERNI / HOTTELIER, Droit constitutionnel suisse, vol. II, Berne, 2006, N 1397 ; TF 1C_201/2012 du 12 décembre 2012 consid. 3.1, destiné à publication, ATF 136 V 117 = RDAF 2011 I 396 et note sur cet arrêt, 120 V 439 consid. 3b, 99 V 15). La doctrine admet toutefois l'utilisation de tels moyens de preuve avec plus ou moins de précision et de restriction (pour une analyse détaillée, cf. TF 1C_201/2012 précité). Ce principe jurisprudentiel est par ailleurs actuellement ancré dans les codes de procédures civile et pénale (art. 152 al. 2 CPC et 141 al. 2 CPP).

6.2 Que ce soit en procédure pénale, civile ou administrative, il y a lieu en tous les cas de procéder à une pesée des intérêts en présence : celui à la manifestation de la vérité, d'une part, celui à la protection du bien lésé par l'obtention illicite, d'autre part (ATF 136 V 117 consid. 4, TF 1C_201/2012 précité ; CHRISTOPH AUER *in* Kommentar zum Bundesgesetz über das Verwaltungsverfahren (VwVG) 2008, n. 23 ad art. 12 ; FRANÇOIS-ROGER MICHELI / CHRISTIAN-NILS ROBERT, Documents volés et dénonciations fiscales, *in* Jusletter 19 novembre 2012, n. 66 ; cf. également art. 152 al. 2 CPC et 141 al. 2 CPP).

6.2.1 La procédure pénale distingue les preuves absolument inexploitables, obtenues par la contrainte, le recours à la force, les menaces, etc. (art. 141 al. 1 CPP), les preuves exploitables, administrées en violation de prescriptions d'ordre, (art. 141 al. 3 CPP) et les preuves relativement inexploitables, soit les preuves administrées d'une manière illicite ou en violation de règles de validité. Concernant ces dernières, elles sont exploitables pour autant qu'elles soient indispensables pour élucider des infractions graves (art. 141 al. 2 CPP). La pesée des intérêts qui est faite consiste dès lors à admettre l'intérêt public à l'utilisation de telles preuves en fonction de la gravité de l'acte (ATF 131 I 272 consid. 4). En effet, plus l'infraction est grave, plus l'intérêt de l'Etat à découvrir la vérité prime sur l'intérêt privé en cause (LUCIE OTTINGER, L'exploitation des moyens de preuve obtenus illégalement : de la situation actuelle à celle du CPP unifié, n. 8 ss, *in* Jusletter 24 août 2009). Le seuil de gravité à franchir n'a expressément pas été défini par le législateur. Le niveau de gravité d'infraction requis devrait logiquement varier en fonction de l'importance des intérêts protégés par la règle violée et de la gravité de l'atteinte qui leur a été portée par les actes de l'autorité (CR CPP - JÉRÔME BÉNÉDICT / JEAN TRECCANI, art. 141 N 25). Le

Tribunal fédéral a notamment considéré que les violations graves d'une règle de la circulation routière, passibles d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire, ne constituaient pas des cas de criminalité dure, précisant que ce sont avant tout les crimes qui entrent dans la catégorie des infractions graves, de sorte que la gravité des infractions litigieuses parlait plutôt en faveur d'une simple interdiction de principe du moyen de preuve obtenu illégalement (ATF 137 I 218 consid. 2.3.5.2 = JT 2011 I 354).

6.2.2 Se référant aux principes précités applicables en procédure pénale, les auteurs François-Roger Micheli et Christian-Nils Robert considèrent qu'en matière fiscale seule l'infraction d'escroquerie aggravée atteint le degré de gravité suffisant pour permettre sa poursuite au moyen de données volées, les autres infractions étant des délits et prévoyant une peine-menace de trois ans de privation de liberté (FRANÇOIS-ROGER MICHELI / CHRISTIAN-NILS ROBERT, op. cit., n. 73 et 74). Ces auteurs relèvent également que les intérêts publics et privés voulant que la justice reflète la vérité matérielle sont sensiblement plus importants dans le domaine pénal que celui de la taxation fiscale, le différend fiscal portant essentiellement sur des enjeux pécuniaires et l'égalité des contribuables, alors que le différend pénal affecte directement la paix sociale, la fonction rétributive de la justice, et cas échéant les intérêts de la victime de l'infraction (n. 70 et 71).

6.3

6.3.1 En l'espèce, l'extension de la surveillance au-delà du 5 novembre et l'analyse effectuée par SCRT à la demande du SDI étaient illicites, comme on l'a vu. Si l'autorité disciplinaire avait été nantie par le SDI, après le premier contrôle de cinq jours, de l'existence de soupçons d'usage abusif d'Internet, elle aurait pu elle-même ordonner l'extension de la surveillance et faire procéder ensuite aux analyses anonymes ou pseudonymes des fichiers journaux permettant de confirmer ou d'infirmer les soupçons, puis, en cas de confirmation, fait procéder aux analyses nominatives en vue d'identifier les auteurs des abus en question. L'autorité disciplinaire aurait alors pu ordonner la saisie de disques durs.

6.3.2 Toutefois, la pesée des intérêts à effectuer ne justifie pas l'utilisation des données résultant des analyses de SCRT effectuées avant la saisie du disque dur du recourant. En effet, il y a tout d'abord lieu de relever que la procédure disciplinaire de la fonction publique a non seulement pour but d'assurer, sur le plan interne, la bonne exécution du travail administratif, mais également de régler les rapports entre l'administration et le public, afin de promouvoir la confiance indispensable à une activité administrative efficace (BOINAY, Le droit disciplinaire dans la fonction publique et dans les professions libérales, particulièrement en suisse romande, *in* RJJ 1998 p. 7). Il est pour le surplus précisé que dans le cas d'espèce ce n'est pas la bonne exécution du travail du recourant qui est mise en cause, mais l'incidence du comportement du recourant sur l'image de l'administration. Il l'ensuit que, à l'instar du différend fiscal, les intérêts de la procédure disciplinaire administrative apparaissent moins importants que ceux d'un différend pénal, ce dont il y a lieu de tenir compte dans la pesée des intérêts.

A cela s'ajoute le fait que la surveillance de novembre 2008, qui aurait certes pu être ordonnée valablement par une autorité compétente, avait pour objectif de confirmer des soupçons d'usage abusif d'Internet, respectivement la consultation de sites à caractère pornographique, pendant et hors du temps de travail. L'usage abusif d'Internet est considéré, dans un cas normal, comme une faute d'importance mineure (cf. TF 8C_448/2012 du 13 janvier 2013 consid. 7.2, destiné à publication, et la référence citée). Il est rappelé qu'une telle analyse porte indiscutablement atteinte à la sphère privée de l'utilisateur concerné (cf. consid. 4.2).

La procédure disciplinaire ouverte à l'encontre du recourant a abouti au constat d'une faute de gravité moyenne et au transfert dans une classe inférieure de traitement durant cinq ans (cf. dossier PER – Enquête disciplinaire N 17, p. 9.12 et 19.5 et PJ 2 recourant). La sanction disciplinaire prononcée se situe du reste au milieu de l'échelle des sanctions prévues à l'article 31 LStMF.

En résumé, l'intérêt de l'autorité disciplinaire à l'établissement de la vérité s'oppose à celui du recourant à bénéficier d'une instruction conforme au droit, respectant la protection de sa sphère privée. Ce dernier intérêt doit être considéré comme prépondérant, d'autant plus que la gravité de la faute qu'on reproche au recourant a été qualifiée de moyenne. Cette pesée des intérêts conduit à une interdiction pure et simple du moyen de preuve obtenu illégalement. Dès lors, pour rendre sa décision, le Gouvernement ne pouvait valablement se fonder sur les analyses effectuées en novembre 2008.

6.3.3 Quant aux preuves recueillies ultérieurement, soit la saisie du disque dur (et les analyses qui ont été faites de ce dernier) ainsi que les déclarations du recourant, bien qu'ordonnées par l'autorité compétente, elles n'auraient pas pu être obtenues sans les résultats d'analyses résultant de la surveillance de novembre 2008, puisque le contrôle des cinq premiers jours de novembre avait uniquement permis de constater des dysfonctionnements dans trois services (…) qui disposent chacun d'une centaine de collaborateurs. Le Gouvernement, en tant qu'autorité disciplinaire, ne pouvait pas, nanti des premiers soupçons résultant de la surveillance des cinq premiers jours de novembre 2008, faire saisir plusieurs centaines de disques durs et les faire analyser. Il devait ordonner au préalable une surveillance des accès à Internet pendant une période à définir puis faire procéder aux analyses voulues.

La doctrine et la jurisprudence ne se sont à l'heure actuelle pas encore expressément prononcées sur la question de savoir si, en procédure administrative, l'interdiction d'utiliser une preuve ne vaut que pour les moyens de preuve primaires obtenus illégalement ou si elle s'étend à tous les autres moyens de preuve qui ont été obtenus au moyen de ces preuves primaires illégales. Le Tribunal fédéral semble admettre un renvoi aux principes applicables en matière pénale (cf. TF 8C_448/2012 précité consid. 6.4.2). En procédure pénale, l'interdiction d'utiliser des preuves illicites s'étend également aux preuves obtenues indirectement (preuves dérivées) lorsque celles-ci n'auraient pas été accessibles sans la preuve originale obtenue illicitement (art. 141

al. 4 CPP ; ATF 138 IV 169 consid. 3.3.1 à 3.3.3 ; 137 I 218 consid. 2.4 ; ATF 133 IV 329 consid. 4.5 ; PIQUEREZ / MACALUSO, Procédure pénale suisse, 3ème éd., N 985). Le Tribunal fédéral a encore précisé qu'il n'y a pas d'effet indirect de l'interdiction d'exploiter la preuve originaire lorsque la seconde preuve aurait aussi pu être obtenue sans la première preuve illicite, avec une grande vraisemblance, compte tenu d'un déroulement hypothétique des investigations. Les circonstances concrètes sont déterminantes. La simple possibilité théorique d'obtenir la preuve de manière licite ne suffit pas (ATF 138 IV 169 consid. 3.3.3).

Il est rappelé que, pour atteindre le but initial, à savoir déterminer la cause des lenteurs et des dysfonctionnements dans l'accès à Internet, des mesures moins attentatoires à la sphère privée que les mesures de surveillance ordonnées, étaient envisageables : un blocage de l'accès à certains sites considérés comme problématiques ou une simple limitation du débit de téléchargement depuis les sites trop gourmands en bande passante aurait suffi à résoudre le problème (Sylvain MÉTILLE, op. cit. n. 11). Le Tribunal fédéral admet également que le blocage préventif de certains sites Internet constitue une mesure adéquate dans le cadre de la lutte contre l'usage abusif des outils informatiques (8C_448/2012 précité consid. 5.5.4). Selon le préposé fédéral à la protection des données, en cas d'utilisation abusive d'Internet, plutôt que surveiller ses employés, l'employeur doit mettre en œuvre les mesures d'ordre technique permettant de contenir les abus et de protéger l'entreprise. Il ne sera autorisé à analyser nominativement les fichiers journaux que si les mesures prises s'avèrent inefficaces et encore faudra-t-il qu'il en ait informé au préalable le personnel dans le cadre du règlement de surveillance. En l'absence d'abus et d'information préalable, il ne pourra analyser les fichiers journaux du surf et du courrier électronique que sous forme anonyme ou pseudonyme (cf. guide relatif à la surveillance de l'utilisation d'internet et du courrier électronique au lieu de travail du Préposé fédéral à la protection des données et à la transparence, p. 4, publié sur le site Internet du Préposé fédéral à la protection des données et à la transparence > Documentation > Brochures > Surveillance de l'utilisation d'Internet et du courrier électronique au lieu de travail). Dans une brochure intitulée : "Protection des données et de la personnalité sur le lieu de travail: un droit légitime" de janvier 2013, le Préposé recommande en cas d'abus de d'abord procéder à une évaluation anonyme, puis d'adresser une mise en garde générale et finalement d'évaluer les données individuellement qu'en cas de récidive et d'irrégularité flagrante (cf. recommandation n° 1). Les directives techniques relatives aux enregistrements et à la surveillance informatique au sein de la République et Canton du Jura du 13 mars 2001 prévoient par ailleurs dans ce sens qu'en cas de manquement aux règles d'utilisation d'Internet l'attention des collaborateurs sera portée sur les types d'utilisation tolérés et ceux qui ne le sont pas, sous la forme d'une communication générale établie à leur intention.

Rien au dossier ne permet d'admettre avec une grande vraisemblance que le Gouvernement, sur la base des résultats de la surveillance des cinq premiers jours de novembre 2008, aurait pris directement la décision d'étendre la surveillance des fichiers journaux à toute l'administration sur une période plus importante, tel que l'a fait le SDI, via la société SCRT, sans respecter la réglementation précitée,

respectivement le principe de la proportionnalité qui implique que soient prises au préalable des mesures moins incisives. En cas d'échec de telles mesures, après évaluation anonyme et toujours dans un souci de prévention, il aurait certainement adressé une mise en garde générale avant d'analyser les données individuellement comme le prévoient les recommandations et directives citées ci-dessus. Dans une telle hypothèse, respectivement en cas de mise en garde claire et sans équivoque portant sur la consultation de sites pornographiques et non pas seulement de sites illégaux au sens de l'article 197 CP, pendant et en dehors du temps de travail, il est possible que le recourant aurait cessé ses activités, ce dernier ayant toujours affirmé qu'il ne se sentait pas concerné par les directives et les avertissements de ses supérieurs dans la mesure où il ne consultait que des sites légaux en dehors de son temps de travail. A supposer toutefois que le recourant passe au-dessus d'une telle mise en garde, et que le Gouvernement étende la surveillance à une période plus importante, les éléments au dossier ne permettent en tous les cas pas de penser que ces investigations auraient permis avec une grande vraisemblance d'arriver à la conclusion que le recourant se livrait à la consultation abusive d'Internet dans la mesure où les analyses effectuées n'ont permis de ne retenir qu'une consultation très occasionnelle des sites prohibés (cf. p. 115 du dossier de la Cour adm.) et il eût fallu que la surveillance porte précisément sur une période où tel avait été le cas.

Ainsi, les analyses effectuées sur la base du disque dur saisi et les déclarations du recourant qui s'en sont suivies, qui n'ont été rendues possibles qu'en raison des premières analyses illicites, doivent être considérées comme des preuves dérivées inexploitables au vu de ce qui précède.

6.3.4 Faute de preuves exploitables, le Gouvernement ne pouvait constater un usage abusif d'Internet de la part du recourant, que ce soit durant ses heures de travail ou en dehors. Partant, il ne pouvait prononcer une quelconque sanction disciplinaire à son encontre.

7. Le recours doit dès lors être admis et la décision du 24 juin 2009 annulée. Il n’est ainsi pas nécessaire d’examiner les autres griefs du recourant, en particulier la violation du droit à un procès équitable au regard des articles 29 Cst et 6 CEDH, 28ss CC ou 26 Cpa.

8. Au vu du sort du recours, les frais de la procédure doivent être laissés à l'Etat (art. 219 Cpa). Le recourant qui obtient gain de cause a droit à une indemnité de dépens, à payer par l'Etat (art. 227 Cpa).

PAR CES MOTIFS
LA COUR ADMINISTRATIVE

admet

le recours ; partant

annule

la décision du Gouvernement du 24 juin 2009 ;

laisse

les frais de la procédure à l'Etat ;

restitue

au recourant son avance de CHF 1000.- ;

alloue

au recourant une indemnité de dépens par CHF 13'000.-, débours et TVA compris, à verser par l'intimé ;

informe

les parties des voies et délai de recours selon avis ci-après ;

ordonne

la notification du présent arrêt :
- au recourant, par son mandataire, Me Jean-Marie Allimann, avocat à 2800 Delémont ;
- à l'intimé, par son mandataire, Me Marco Locatelli, avocat à 2800 Delémont.

Porrentruy, le 25 février 2013

AU NOM DE LA COUR ADMINISTRATIVE

Le président :	**La greffière :**
Pierre Broglin	Nathalie Brahier

Communication concernant les moyens de recours :

*Le présent arrêt peut faire l'objet, **dans les trente jours** suivant sa notification, d'un recours au Tribunal fédéral. Le recours en matière de droit public s'exerce aux conditions des articles 82 ss de la loi du 17 juin 2005 sur le Tribunal fédéral (LTF - RS 173.110), le recours constitutionnel subsidiaire aux conditions des articles 113 ss LTF. Le*

mémoire de recours doit être adressé au Tribunal fédéral, Schweizerhofquai 6, 6004 Lucerne ; il doit être rédigé dans une langue officielle, indiquer les conclusions, les motifs et les moyens de preuve, et être signé. Les motifs doivent exposer succinctement en quoi l'acte attaqué viole le droit. Si le recours n'est recevable que s'il soulève une question juridique de principe, il faut exposer en quoi l'affaire remplit cette condition. Les pièces invoquées comme moyens de preuve doivent être jointes au mémoire, pour autant qu'elles soient en mains de la partie; il en va de même de la décision attaquée.