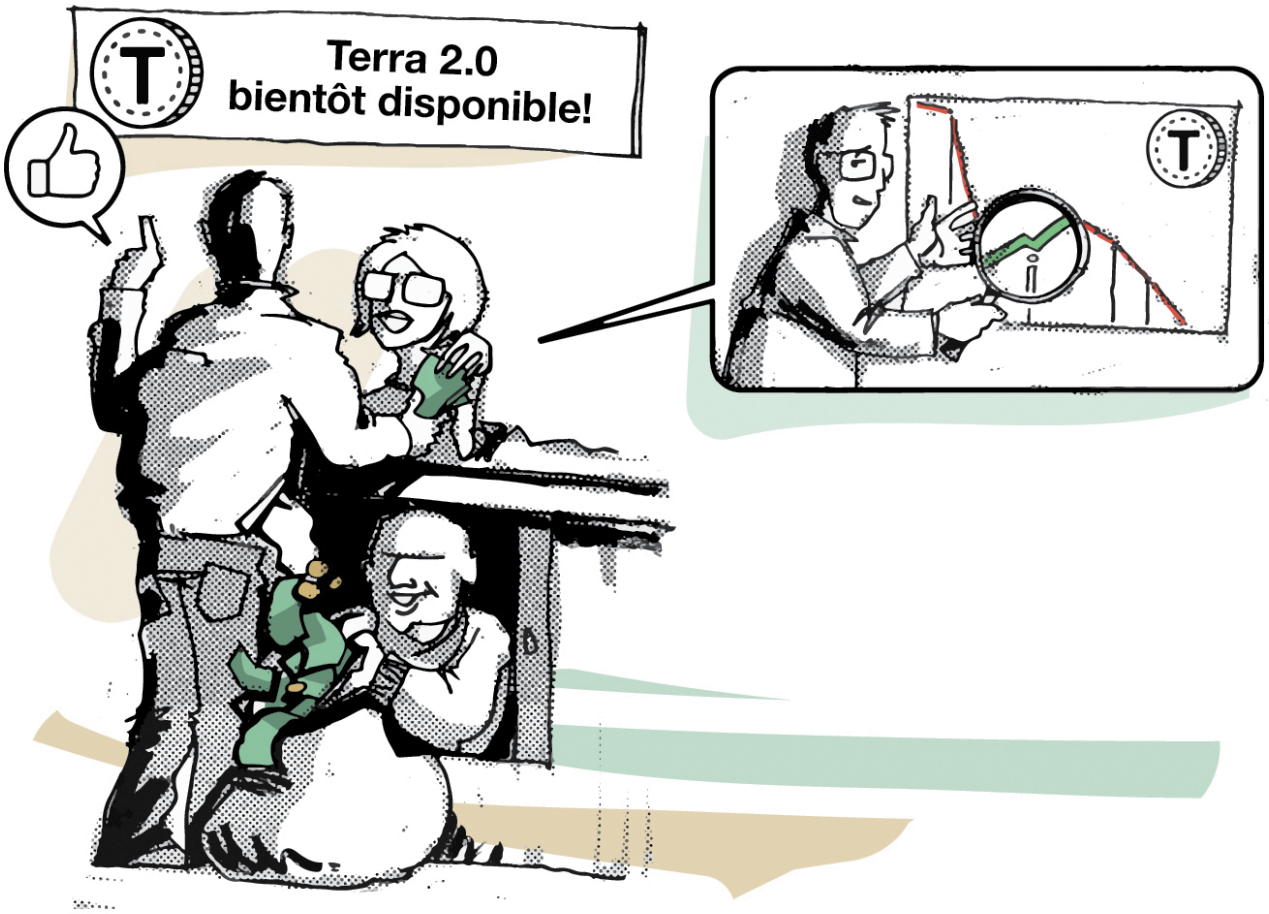
GENEVA INTERNET PLATFORM
digwatch

LETTRE D'INFORMATION

Numéro 70 – juin 2022



Le marché des crypto-monnaies en danger ?

Pages 2–3

TENDANCES

La politique en matière de contenus en ligne, le krach du marché des crypto-monnaies et les questions numériques à l'ordre du jour des ministres du Numérique du G7, de la CTT et du Quad.

Pages 2–3

NIS2

Un accord politique sur la NIS2 de l'UE a été conclu. Nous examinons son contexte, ses principales composantes et les prochaines étapes de son parcours législatif.

Pages 6–7

LE NUMÉRIQUE À DAVOS

Les sujets numériques ont été au cœur de l'ordre du jour de la réunion annuelle du Forum économique mondial (WEF), qui s'est tenue à Davos. Voici ce qui a été discuté.

Page 10

GENÈVE

De nombreux débats politiques ont lieu chaque mois à Genève. Tenez-vous au courant des dernières nouvelles de la Genève internationale.

Page 11

ORGANISATION INTERNATIONALE DE la francophonie

D-CLIC FORMEZ-VOUS AU NUMÉRIQUE !

La lettre d'information en français *Digital Watch* est publiée en collaboration et avec le soutien de l'Organisation internationale de la Francophonie dans le cadre de l'initiative D-CLIC, Formez-vous au numérique avec l'OIF.

Principales tendances en matière de politique numérique

1. Politique de contenu en ligne

Le 14 mai, Payton Gendron aurait tué dix personnes et en aurait blessé trois autres lors d'une fusillade de masse dans une épicerie de Buffalo.

Deux jours auparavant, un manifeste qu'il aurait rédigé avait été publié dans Google Docs, décrivant le plan de la fusillade et affirmant qu'il avait été **radicalisé sur 4chan** – un tableau d'affichage basé sur des images, avec des contributeurs anonymes.

Gendron **a créé un salon de discussion privé sur l'application de communication Discord**, qui lui servait de journal de discussion personnel. Il a diffusé l'attaque sur la plateforme de diffusion en continu (*streaming*) Twitch, qui a affirmé avoir **retiré la vidéo dans les deux minutes suivant le début de l'attaque**. Cependant, un enregistrement de la vidéo a été rapidement **mis en ligne sur Streamable**, un autre site de *streaming*.

Des **liens vers l'enregistrement ont été partagés sur Facebook et Twitter**, qui ont eu du mal à le contenir. Certains utilisateurs qui avaient signalé la vidéo sur Facebook ont été informés qu'elle **ne violait pas ses règles**. Plusieurs usagers ont signalé qu'une séquence qui montrait le tireur tirant sur des personnes avait **été visible et vue sur Twitter pendant quatre heures**. Des utilisateurs de TikTok auraient téléchargé des vidéos partageant des comptes et des termes de **recherche pour amener les spectateurs à la vidéo complète sur Twitter**.

La fusillade de Buffalo **a renforcé les appels à la responsabilisation des plateformes en ligne**. Twitch, Discord et 4chan font l'objet d'une **enquête du procureur général de New York** concernant leur rôle dans la promotion de la violence. Le New Jersey a lancé **une enquête similaire sur Twitch et Discord**.

Le monde était encore sous le choc de la nouvelle de la fusillade de Buffalo lorsque Salvador Ramos tuait 21 personnes et en blessait 19 autres lors d'une fusillade de masse dans une école primaire d'Uvalde, au Texas, le 24 mai. Les rapports suggèrent que Ramos a posté sur Instagram des **photos des deux armes à feu qu'il a utilisées** lors de l'attaque, le 20 mai. Meta, la société mère d'Instagram et de Facebook, ne limite pas les photos ou les *hashtags* autour des armes à feu, ce qui rend la détection plus difficile. Comme la légende de la publication Instagram indiquait « Les enfants ont peur » et n'appelait pas plus à la violence, elle n'a pas été repérée. L'enquête qui a suivi a indiqué que, quelques minutes avant l'attaque, Ramos avait envoyé des **messages privés sur Facebook** annonçant qu'il allait tirer sur une école primaire.

Ces événements ont alimenté un débat en cours sur la responsabilité des médias sociaux en matière de contenus en ligne et de liberté d'expression aux États-Unis. La Cour suprême des États-Unis était **sur le point de se prononcer** à propos de la mise en œuvre de la **loi texane sur les médias sociaux**, qui interdit aux plateformes de médias sociaux comptant au moins 50 millions d'utilisateurs actifs de bloquer, supprimer ou « démonétiser » des contenus en fonction des opinions des utilisateurs. Cette loi rendrait **illégale la suppression** par les grandes plateformes de médias sociaux du contenu posté par les tireurs. Les entreprises technologiques ont déposé un appel d'urgence juste après la fusillade de Buffalo, soulignant les arguments pour bloquer cette loi. Le 31 mai 2022, la Cour suprême des États-Unis s'est rangée du côté de l'industrie technologique et a **bloqué la loi controversée du Texas**. Un débat sur les discours haineux et le retrait des contenus s'est également conclu dans l'UE, dans le cadre des négociations de la loi sur les services numériques. **Les très grandes plateformes en ligne** sont tenues de retirer « immédiatement » les contenus ciblant les victimes de la cyber-violence, et les autres contenus jugés illégaux doivent être retirés « rapidement ». Nous avons parlé plus en détail de **la loi sur les services numériques** dans notre bulletin d'information du mois dernier.

Les événements tragiques du mois de mai soulèvent d'importantes questions politiques : l'Appel de Christchurch visant à éliminer le contenu terroriste et extrémiste violent en ligne sera-t-il renforcé ou une nouvelle initiative verra-t-elle le jour ? Va-t-on assister à un renforcement des politiques visant à rendre plus difficile le téléchargement de vidéos violentes sur les plateformes en ligne ? Ou verrons-nous des appels à un cryptage plus faible des conversations privées ?

La fusillade de Christchurch a conduit à la création de **l'Appel de Christchurch** lorsque plusieurs gouvernements et plateformes en ligne ont promis d'intensifier leurs efforts pour éliminer les contenus terroristes et extrémistes violents en ligne. Le responsable de l'Appel de Christchurch affirme que ses outils ont rendu plus difficile la diffusion virale de la vidéo de la fusillade de Buffalo.

2. Le marché des crypto-monnaies en danger

La populaire crypto-monnaie stable Terra a survécu à un effondrement total en mai : la pièce de monnaie cryptographique Luna (liée à l'écosystème Terra), qui s'échangeait à 110 dollars, est tombée à 0,05 dollar le lendemain, effaçant près de 50 milliards de dollars de valeur. Cette rupture majeure a sonné l'alarme auprès des investisseurs et des régulateurs du monde entier. Beaucoup ont soupçonné qu'il s'agissait peut-être de la fin de l'engouement pour les

crypto-monnaies, étant donné que toutes les entreprises technologiques ont connu des difficultés et une baisse du prix des actions. Mais les crypto-monnaies se tiennent toujours à peu près au même niveau. La pièce Terra fait l'objet d'une réfutation, tandis que plusieurs Bourses de crypto-monnaies ont annoncé qu'elles commenceront à négocier la Terra 2.0 dès qu'elle sera disponible.

Que sont les crypto-monnaies stables ? Pourquoi Terra a-t-elle été si populaire parmi les investisseurs ? Comment pouvons-nous protéger les investisseurs et les clients ? Pour en savoir plus, lisez les pages 8 et 9.

3. Le numérique dans la haute politique

Ce mois-ci, la politique numérique était à l'ordre du jour des ministres du G7 chargés du Numérique, du Conseil américano-européen du commerce et des technologies (TTC), et du sommet des dirigeants de la Quadrilatérale.

Les ministres du Numérique du G7. Lors **de leur réunion à Düsseldorf** les 10 et 11 mai 2022, les ministres du Numérique des pays du G7 ont **réitéré leur engagement** à « déployer des efforts concertés pour maintenir un Internet libre, mondial, ouvert, interopérable, fiable et sécurisé qui soutient l'innovation et renforce le respect des valeurs démocratiques et des droits de l'Homme universels ». Ils ont adopté **un plan d'action** pour **promouvoir la libre circulation des données en toute confiance (DFFT)**, ainsi qu'un ensemble de principes pour les cadres juridiques nationaux visant à promouvoir l'utilisation des documents électroniques transférables. **Une déclaration commune sur la cyber-résilience des infrastructures numériques en réponse à la guerre russe contre l'Ukraine** a été publiée, soulignant l'engagement du G7 à accroître la cyber-résilience des infrastructures numériques et à continuer à soutenir l'Ukraine dans la défense de ses réseaux contre les cyber-incidents.

CCT (Conseil du commerce et des technologies) UE-US. Les principaux résultats de la **deuxième réunion ministérielle du CCT UE-États-Unis** du 16 mai sont les suivants :

- le lancement d'un mécanisme d'information stratégique sur la normalisation destiné à faciliter l'échange d'informations sur l'élaboration de normes internationales ;
- la création d'un sous-groupe sur l'intelligence artificielle chargé d'élaborer une feuille de route sur les outils d'évaluation et de mesure pour une intelligence artificielle digne de confiance, ainsi qu'un projet sur les technologies d'amélioration de la vie privée ;
- la création d'un dialogue politique sur les questions liées à la modération des contenus, et l'engagement de développer un cadre analytique commun pour identifier la « manipulation et l'interférence des informations étrangères », qui devrait permettre de prendre des contre-mesures efficaces ;
- la création d'un sous-groupe de travail chargé de développer une compréhension commune des pénuries de semi-conducteurs et de faciliter la coordination dans ce domaine ;
- le lancement d'un groupe de travail sur le financement public de la connectivité sûre et résiliente et des chaînes d'approvisionnement des technologies et services d'information et de communication (TICS) dans les pays tiers, afin de promouvoir le recours à des « fournisseurs de confiance / non à haut risque » et de faciliter la collaboration sur le financement public États-Unis-UE de projets TICS dans les pays tiers, sur la base de principes communs.

Sommet des dirigeants de la Quadrilatérale. Le 24 mai, les Premiers ministres de l'Australie, de l'Inde et du Japon, ainsi que le président des États-Unis se sont réunis à Tokyo pour le deuxième sommet **des dirigeants de la Quadrilatérale**, et **ont convenu** de ce qui suit :

- approfondir la collaboration et mener des actions complémentaires dans le domaine de la connectivité numérique ;
- coopérer pour améliorer la défense de leurs infrastructures critiques ;
- coordonner les programmes de renforcement des capacités en matière de cybersécurité dans la région indo-pacifique, dans le **cadre du partenariat quadrilatéral** pour la cybersécurité ;
- faire progresser l'interopérabilité et la sécurité dans la 5G et au-delà de la 5G en signant un nouveau protocole de coopération sur la diversification des fournisseurs de la 5G et l'Open RAN ;
- faire progresser la coopération sur les semi-conducteurs et d'autres technologies critiques, et renforcer la résilience face à divers risques (**une déclaration de principes commune sur les chaînes d'approvisionnement en technologies critiques a été publiée**, énumérant la sécurité, la transparence, l'autonomie et l'intégrité comme principes volontaires pour aider les gouvernements et les organisations à prendre des décisions concernant leurs fournisseurs et la sécurité de leurs produits) ;
- renforcer la coopération au sein des organisations internationales de normalisation ;
- approfondir les discussions et la coopération sur les questions liées à la biotechnologie et aux technologies quantiques.

Les développements de la politique numérique qui ont fait la une

Le paysage de la politique numérique évolue quotidiennement. Voici donc les principaux développements du mois de mai. Nous les avons décodés en petites mises à jour qui font autorité. Vous trouverez plus de détails dans chaque mise à jour sur le Digital Watch Observatory.

En hausse

Architecture de gouvernance numérique mondiale

Le Secrétariat des Nations unies a lancé une consultation publique sur les éléments à inclure dans le Pacte mondial pour le numérique.

En baisse

Le développement durable

L'UE et le Japon ont lancé un partenariat numérique pour favoriser la croissance économique et parvenir à une société durable. La Commission économique et sociale des Nations unies pour l'Asie et le Pacifique a publié des documents explorant l'intersection de la connectivité et de l'économie numérique et le statut de la connectivité transfrontalière en Asie du Sud-Est.

En hausse

La sécurité

Le deuxième protocole additionnel à la Convention de Budapest sur la cybercriminalité a été ouvert à la signature.

Le Costa Rica a déclaré l'état d'urgence national à la suite des attaques par rançongiciel (*ransomware*) de Conti. Plus tard, des chercheurs ont indiqué que Conti mettait fin à ses activités et se réorganisait.

Les États-Unis, l'UE, le Canada et le Royaume-Uni ont attribué la cyberattaque de Viasat à la Russie. Le collectif d'hacktivistes Anonymous a déclaré la cyberguerre contre Killnet, un groupe de hackers pro-russes. Killnet a lui-même déclaré la cyberguerre à dix pays. Les opérations de rançongiciels REvil semblent avoir repris.

La Commission européenne a lancé une stratégie pour un meilleur Internet pour les enfants et une proposition législative contre le matériel d'exploitation sexuelle des enfants.

En hausse

Le commerce électronique et l'économie de l'Internet

La Commission européenne a fait valoir qu'Apple avait abusé de sa position dominante dans le domaine des portefeuilles mobiles sur iOS. Le Royaume-Uni cherche à déterminer si les pratiques de Google sur le marché de la technologie publicitaire sont anticoncurrentielles.

Le Japon a adopté une loi historique sur la réglementation des monnaies stables. La République centrafricaine a annoncé son intention de lancer une plateforme d'investissement en crypto-monnaies. L'Ouzbékistan a exempté les opérations de crypto monnaies de l'impôt sur le revenu.

En baisse

L'infrastructure

Le Canada a annoncé un plan visant à bannir Huawei et ZTE des réseaux 4G et 5G.

L'OMPI a suspendu les services de règlement des litiges relatifs aux noms de domaine en « .ua ».

Les droits numériques

En baisse

La Commission européenne **a présenté des propositions pour un espace européen** des données de santé.

Meta a **réécrit et remanié sa politique de confidentialité**, accompagnée d'un **nouvel outil** permettant aux utilisateurs de définir un public par défaut pour leurs publications. Le district américain de Columbia **poursuit Mark Zuckerberg pour des violations de la vie privée** dans le cadre du scandale Cambridge Analytica.

Des **perturbations de l'Internet** ont été enregistrées au Pakistan dans le cadre de manifestations publiques.

Les politiques de contenu

En hausse

La Cour suprême des États-Unis **a bloqué une loi controversée du Texas** qui interdit aux plateformes de médias sociaux comptant au moins 50 millions d'utilisateurs actifs de bloquer, supprimer ou démonétiser des contenus sur la base des opinions des utilisateurs.

L'Autriche a lancé **un plan d'action pour lutter** contre les fausses informations (*deepfakes*).

Elon Musk **reste attaché à l'acquisition de Twitter**, mais a exigé que Twitter démontre que **les comptes de spam représentent moins de 5 % de l'ensemble des comptes Twitter** pour que l'opération puisse se poursuivre. Le conseil d'administration de Twitter a déclaré qu'il prévoyait de **« conclure la transaction et d'appliquer l'accord de fusion » entre Musk et Twitter**. L'affaire est maintenant **entre les mains de la SEC**, qui doit approuver l'offre de Musk de racheter Twitter (qui est cotée en Bourse).

La juridiction et les questions juridiques

En baisse

De grandes entreprises technologiques sont poursuivies en Russie **pour avoir retiré leurs services du pays**.

L'agence espagnole de protection des données a infligé **une amende de 10 millions d'euros à Google** pour des infractions au GDPR.

Google a annoncé **avoir conclu des accords de licence de contenu avec plus de 300 éditeurs en Europe**, conformément à la directive de l'UE sur le droit d'auteur.

Les nouvelles technologies

En hausse

L'Irlande **a nommé son premier ambassadeur de l'intelligence artificielle**. Singapour **a lancé un cadre de test de l'IA**. Des groupes de la société civile ont appelé le Parlement européen **à interdire la surveillance biométrique**. Le gouvernement américain **a mis en garde contre les discriminations liées au handicap causées par les outils d'IA utilisés pour prendre des décisions en matière d'emploi**.

Clearview AI a accepté **de cesser de vendre son logiciel de reconnaissance faciale à des entreprises privées aux États-Unis**. Au Royaume-Uni, l'entreprise a reçu l'ordre **de supprimer les données appartenant à des résidents britanniques**.

Le président américain a publié **un mémorandum sur la sécurité nationale** et un **décret visant** à assurer le *leadership* des États-Unis dans le domaine de la science de l'information quantique et à atténuer les risques associés aux ordinateurs quantiques. Des chercheurs de l'université de technologie de Delft **ont annoncé des avancées vers un futur Internet quantique**.

La directive NIS2

Le 13 mai, le Parlement et le Conseil européens sont parvenus à un accord politique sur une directive concernant des mesures visant à assurer un niveau commun élevé de cybersécurité dans l'Union, communément appelée NIS2. Nous abordons le contexte du document, ses principales composantes et les prochaines étapes de son parcours législatif.

Contexte

La Commission de l'UE a adopté en décembre 2020 une proposition de directive révisée sur la sécurité des systèmes de réseaux et d'information « afin d'améliorer encore les capacités de résilience et de réaction aux incidents des entités publiques et privées, des autorités compétentes et de l'Union dans son ensemble dans le domaine de la cybersécurité et de la protection des infrastructures critiques ». La directive révisée, connue sous le nom de NIS2, s'appuie sur la directive relative à la sécurité des réseaux et des systèmes d'information (NIS1), adoptée en 2016, première législation européenne en matière de cybersécurité, qui prévoit des mesures juridiques visant à renforcer le niveau global de cybersécurité dans l'UE.

Buts et objectifs

Selon la proposition de la Commission européenne, la directive NIS2 vise à réorganiser et à actualiser le cadre juridique existant tout en tenant compte de la numérisation rapide du marché intérieur de l'UE et du paysage croissant des menaces pour la cybersécurité que la pandémie de COVID-19 a encore intensifié.

En outre, la directive NIS2 comble quelques lacunes qui ont empêché la directive NIS de déployer tout son potentiel. L'évaluation de la directive NIS1 par la Commission européenne a révélé les lacunes suivantes :

1. le faible niveau de cyber-résilience des entreprises opérant dans l'UE ;
2. une résilience inégale entre les États membres et les secteurs ;
3. le faible niveau de connaissance commune de la situation et l'absence de réponse commune aux crises.

Secteurs concernés

L'un des principaux changements de la directive NIS2 est qu'elle ne fait pas de distinction entre les opérateurs de services essentiels et les fournisseurs de services numériques. La NIS2 élargit considérablement les secteurs d'activité et les répartit en deux catégories, énumérées à l'annexe I et à l'annexe II de la directive. Tous deux doivent se conformer aux exigences de gestion du risque de cybersécurité et aux obligations de déclaration.

- **Les secteurs essentiels** comprennent la santé, l'énergie, les transports, les banques et les infrastructures numériques, ainsi que les secteurs de l'administration publique et de l'espace.
- **Les secteurs importants** comprennent les entités fabriquant des dispositifs médicaux, les services postaux, la gestion des déchets, la production et la transformation des aliments, et les fournisseurs numériques.

En revanche, en ce qui concerne la supervision et la mise en œuvre, la procédure diffère selon qu'il s'agit de secteurs essentiels ou importants. Les États membres sont tenus de s'assurer que les mesures imposées aux entités des secteurs essentiels sont efficaces et proportionnées, et ils ont le pouvoir d'effectuer des inspections sur place ou des audits réguliers ciblés sur la base d'évaluations des risques, entre autres. Au contraire, les entités importantes ne font l'objet d'une enquête que si des preuves de non-conformité apparaissent.

Comme pour la NIS1, les micro et petites entités sont exclues du champ d'application de la NIS2.

Secteurs NIS2. Source de l'image : jtsec.es

Les nouveautés de la NIS2

Voici une liste non exhaustive d'exigences NIS2 réparties en quatre catégories.

Cadres réglementaires coordonnés en matière de cybersécurité. Comme la NIS1, la NIS2 oblige les États membres de l'UE à adopter des stratégies nationales de cybersécurité qui doivent définir, entre autres, des objectifs stratégiques, un cadre de gouvernance et des mesures pour assurer la préparation. La NIS2 oblige les États membres de l'UE à mettre en place des équipes de réponse aux incidents de sécurité informatique (CSIRT), qui doivent également faire office de coordinateurs pour la divulgation des vulnérabilités. La NIS2 charge l'Agence de l'Union européenne pour la cybersécurité (ENISA) de développer un registre européen des vulnérabilités, qui devrait comprendre des informations sur les vulnérabilités, les produits et services TIC concernés, et la gravité des vulnérabilités, entre autres.

Coopération. La NIS2 envisage l'établissement formel d'un réseau européen d'organisations de liaison en cas de cyber-crises (EU-CyCLONe) pour « soutenir la gestion coordonnée des incidents et des crises de cybersécurité à grande échelle sur le plan opérationnel, et assurer l'échange régulier d'informations entre les États membres et les institutions de l'UE ». Afin d'évaluer l'efficacité des politiques de cybersécurité des États membres de l'UE et la mise en œuvre des exigences en matière de gestion des risques de cybersécurité et des obligations de déclaration, la Commission européenne mettra en place des examens par les pairs.

Dispositifs de partage d'informations sur la cybersécurité. La NIS2 met l'accent sur le partage d'informations et exige des États membres de l'UE qu'ils veillent à ce que les organisations échangent entre elles des informations pertinentes en matière de cybersécurité, telles que des informations relatives aux cybermenaces, aux vulnérabilités, aux indicateurs de compromission, aux tactiques, techniques et procédures, aux alertes de cybersécurité et aux outils de configuration. En outre, les États membres sont également encouragés à soumettre des notifications volontaires d'incidents ou de cybermenaces importants.

Gestion du risque de cybersécurité et obligations de déclaration. La NIS2 exige que les États membres de l'UE veillent à ce que « les entités essentielles et importantes prennent des mesures techniques et organisationnelles appropriées et proportionnées pour gérer les risques posés à la sécurité des réseaux et des systèmes d'information que ces entités utilisent dans le cadre de la fourniture de leurs services ». Ces mesures comprennent l'analyse des risques et les politiques de sécurité des systèmes d'information, le traitement des incidents, la continuité des activités et la gestion des crises, la sécurité de la chaîne d'approvisionnement, la politique et les procédures (tests et audits) visant à évaluer l'efficacité des mesures de gestion des risques liés à la cybersécurité, ainsi que l'utilisation de la cryptographie et du cryptage. En outre, les États membres de l'UE sont tenus de prendre toutes les mesures coercitives nécessaires pour mettre en conformité le service qui ne respecte pas ces exigences.

Contrairement à la NIS1, la NIS2 exige que les États membres veillent à ce que les entités essentielles et importantes signalent tout incident susceptible d'entraîner une perturbation opérationnelle ou des pertes financières. Les entités doivent informer les autorités compétentes ou les CSIRT de l'événement dans les 24 heures. De plus, il est demandé aux entités de se conformer aux systèmes européens de certification en matière de cybersécurité.

Sanctions

Selon la NIS2, les États membres de l'UE sont chargés de fixer les règles relatives aux sanctions applicables aux infractions aux dispositions nationales. Les organisations qui ne se conforment pas à ces règles pourraient **se voir infliger** une amende maximale de 10 millions d'euros ou de 2 % du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu.

Les étapes suivantes

L'accord provisoire doit maintenant **être approuvé** par les co-législateurs, le Conseil européen et le Parlement européen. La France, qui assure la présidence du Conseil, devrait bientôt soumettre l'accord au Comité des représentants permanents du Conseil pour approbation. Les États membres de l'UE disposeront de 18 mois pour transposer la NIS2 dans leurs législations nationales.

Les crypto-monnaies stables sont-elles un danger pour la crypto-économie ?

La crypto-monnaie stable Terra a survécu à un effondrement total en mai. Qu'est-ce qu'une crypto-monnaie stable ? Pourquoi Terra était-elle si populaire parmi les investisseurs ? Comment protéger les investisseurs et les clients ?

Crypto-monnaie stable et implications pour l'industrie de la cryptographie

Nous pensons souvent que les crypto-monnaies attirent un flux constant d'investissements dans la mesure où leur valeur augmente en permanence. Cependant, un type de crypto-monnaie joue un rôle différent dans son écosystème. Elle a tendance à avoir un prix stable de 1 dollar par pièce. En d'autres termes, elle est rattachée à la monnaie américaine et est appelée *stablecoin*. Les crypto-monnaies stables (*stablecoin*) sont nécessaires au fonctionnement des technologies de finance décentralisée (DeFi) et au bon fonctionnement des échanges en ligne. Dans le DeFi, les crypto-monnaies stables sont utilisées comme garantie, et les échanges en ligne les utilisent pour les règlements mutuels. La plus connue des crypto-monnaies stables, Tether, est souvent considérée comme l'une des raisons de la croissance rapide et explosive des échanges en ligne.

L'histoire de Terra

Il existe deux types très différents de crypto-monnaies stables. Le premier est adossé à des dollars américains (ou, dans certains cas, à un panier de devises), ce qui signifie que chaque crypto-monnaie stable émise a son équivalent analogique stocké dans une chambre forte. Cela offre aux investisseurs la sécurité de convertir leur richesse en jetons numériques et limite la crainte de krachs instantanés du marché, qui se produisent souvent dans le commerce cryptographique. Sachant que les personnes ne conserveront pas longtemps les crypto-monnaies stables, le deuxième type de crypto-monnaie stable – les crypto-monnaies stables dites « algorithmiques » – offre une récompense assez importante pour le jalonnement. Le jalonnement est similaire à la détention d'un compte d'épargne à terme fixe dans une banque ; la version cryptographique offre jusqu'à 20 % de bénéfice si vous ne transférez pas vos monnaies pendant un certain temps. Ils utilisent des algorithmes pour acheter/vendre afin d'équilibrer la valeur de la pièce à 1 dollar. La star de la montée en puissance promise des crypto-monnaies stables était construite par le programmeur sud-coréen Kwon Do-hyung, plus connu sous le nom de Do Kwon. Il a créé l'écosystème Terra avec le TerraUSD natif et les jetons Luna qui ont été émis sur le réseau. Un changement important par rapport aux autres monnaies stables algorithmiques était que Terra devait maintenir son ancrage au dollar américain en utilisant le prix du bitcoin comme principal facteur d'équilibrage. **Do Kwon** est apparu dans les médias du monde entier. L'idée a été propagée comme une « monnaie pour un nouveau système monétaire basé sur le bitcoin, plutôt que sur les monnaies fiduciaires ». Cette remarquable promesse d'un rendement de 20 % pour la période de 12 mois était un piège pour les petits investisseurs ou les retardataires qui poussaient leurs portefeuilles dans ces groupement verrouillés d'où le *stablecoin* tirait sa liquidité. On a estimé que l'écosystème Terra valait plus de 18 milliards de dollars.

Tout semblait assez stable (jeu de mots) pour la nouvelle ère cryptographique, à l'exception d'un petit détail : l'idée que le prix du bitcoin allait augmenter régulièrement et ne jamais baisser - disons 25 % en deux jours. Au vu de l'histoire, c'était une supposition naïve, car c'est exactement ce qui s'est passé. La chute brutale du prix a déclenché une ruée sur la banque, les investisseurs ayant entraîné TerraUSD dans une spirale fatale, perdant 99,8 % de sa valeur.

Les réserves s'épuisaient rapidement, gérées par des techniciens plutôt que par des virtuoses de la finance qui comprenaient la Bourse et les mouvements du marché. D'autres fonds étaient bloqués et inaccessibles. Cela a marqué la fin de l'étoile montante la plus prometteuse du monde des crypto-monnaies. En une brève explosion, TerraUSD a effacé plus de 50 milliards de dollars d'investissements, faisant craindre un effondrement de l'ensemble du marché des crypto-monnaies. Do Kwon fait l'objet d'une investigation du bureau du procureur du district sud de Séoul, qui enquêtera sur Terraform Labs, l'organisation à l'origine du projet *Terra stablecoin*. L'**affaire** a été confiée à son équipe d'enquête conjointe sur les crimes financiers et les délits boursiers.

Dans une déclaration du cabinet d'avocats engagé par les cinq investisseurs portant plainte contre Terraform Labs, il a été déclaré : « La conception et l'émission de Luna et Terra pour attirer les investisseurs, mais le fait de ne pas les informer correctement des défauts, et l'expansion illimitée de l'émission de Luna équivalent à une fraude des investisseurs. » Et c'est effectivement une idée importante que nous devons aborder si nous voulons voir une introduction significative des économies de crypto-monnaies dans la finance régulière.

L'idée des *stablecoins* algorithmiques a été sérieusement ébranlée, mais ce n'est certainement pas la fin des crypto-monnaies. L'effondrement de l'écosystème de Terra raconte une autre histoire sur la cupidité et la volonté de jouer avec l'argent des investisseurs (**Bitconnect**, **OneCoin**, etc. : la liste est longue).

Les autres crypto-monnaies stables

L'explosion des crypto-monnaies stables a commencé en 2020-2021. D'une évaluation de 6 milliards de dollars au 31 décembre 2019, le montant des fonds est passé à 181 milliards de dollars en mai 2022 (**selon les métriques de cryptoblock**). La plus grosse crypto-monnaie stable sur le marché est le Tether, basé aux États-Unis. *Tether Holding Limited*, la société derrière la crypto-monnaie Tether, a jusqu'à présent émis plus de 70 milliards de jetons (équivalant à 70 milliards de dollars), **et elle offre un aperçu quotidien de ses réserves**. Selon l'entreprise, tous les 70 milliards de dollars sont échangeables en monnaies fiduciaires et stockés dans des coffres-forts. La cryptomonnaie Tether est souvent citée comme l'une des principales raisons de l'essor des Bourses mondiales de crypto-monnaies, car elles utilisent Tether comme outil de règlement mutuel. Néanmoins, le Tether a toujours été sous le regard suspicieux des investisseurs et de l'industrie cryptographique. Ces inquiétudes ont été levées en 2021, lorsque la *Commodity Futures Trading Commission* (CFTC) des États-Unis a mené une enquête et publié une déclaration selon laquelle Tether ne disait pas toute la vérité. *Tether Holdings Limited* s'est vu infliger une amende de 41 millions de dollars. La CFTC a déclaré qu'une amende avait été infligée « **pour avoir fait des déclarations fausses ou trompeuses et des omissions de faits importants en rapport avec le jeton Tether (USDT) en dollars américains** ». Cette décision a créé un malaise supplémentaire pour l'ensemble du secteur et **a poussé les régulateurs** à accélérer les travaux sur le cadre dans lequel les crypto-monnaies stables peuvent être contrôlées rapidement et efficacement.

Réglementation des crypto-monnaies stables

Ce n'est pas la première fois que les crypto-monnaies stables sont sous le feu des projecteurs réglementaires. En 2019, Facebook a annoncé qu'il allait créer une crypto-monnaie stable sous le nom de Libra. Ils ont annoncé qu'elle serait arrimée à un panier de devises internationales. Cela a soulevé une réponse importante de la part des régulateurs américains et mondiaux, ce qui a incité le Conseil de stabilité financière (FSB) du G7 à élaborer une stratégie pour la poursuite de la réglementation des crypto-monnaies stables. Le FSB travaille sur la réglementation mondiale des crypto-monnaies stables, car elles sont considérées comme le principal adversaire des monnaies numériques des banques centrales (CBDC), dont la création est déjà en cours.

Le travail sur les lois de protection des consommateurs et l'éducation générale autour des crypto-monnaies devraient être les premières étapes vers un avenir fondé sur les crypto-monnaies. Ce dont nous avons besoin, c'est d'un cadre réglementaire clair qui protégera les investisseurs et permettra une croissance régulière. Dans le cadre de l'effort conjoint pour parvenir à un cadre réglementaire optimal, le gouvernement japonais a présenté la première loi au monde traitant de la question des crypto-monnaies stables. Dans cette nouvelle proposition, **le Japon demandera aux émetteurs de crypto-monnaies stables** « un lien obligatoire avec le yen et [de consacrer] le droit de les racheter à leur valeur nominale ».

Il s'agit d'un premier pas vers une réglementation mondiale, mais il doit être suivi de décisions informatives de la part des régulateurs et des acteurs du marché.

À l'avenir, le mélange de la technologie et de la finance sera plus difficile à réaliser, car ce domaine est sensible à toute forme d'erreur ou d'omission. Tous ces éléments seront rapidement et impitoyablement exploités par les financiers, qui sont dans ce jeu depuis bien plus longtemps que la communauté technologique. Comment créer un environnement efficace, mais sûr, est la principale question dans ce domaine.

Le numérique à Davos

La réunion annuelle phare du Forum économique mondial (WEF) s'est tenue à Davos du 22 au 26 mai. Les dirigeants se sont réunis dans un contexte nouveau « caractérisé par l'émergence d'un monde multipolaire à la suite de la pandémie et de la guerre ». La guerre en Ukraine a occupé le devant de la scène, tandis que les sujets numériques ont été au cœur de l'ordre du jour chargé de la réunion. Voici ce qui a été discuté.

Le krach du marché des crypto-monnaies a fait en sorte qu'elles figurent en bonne place dans l'agenda de Davos. Les critiques sont apparues en force pour discuter de leur avenir et des monnaies numériques des banques centrales. Il a également été question de l'économie quantique, des compromis qui émergent dans l'économie numérique pour les entreprises, de la nécessité de garantir un commerce numérique innovant et ouvert grâce aux services numériques, de l'avenir du commerce de détail et de l'avenir du travail.

Les technologies de pointe, l'IA, les métavers, la santé numérique, la cybersécurité, la réalité augmentée, l'inclusion numérique, le numérique et le climat, la gouvernance des données et la lutte contre les contenus préjudiciables en ligne ont également été abordés.

L'avenir de l'Internet a été examiné, notamment la manière d'utiliser l'approche multipartite pour prévenir un futur *splinternet*, instaurer la confiance dans l'ère numérique et faire progresser la coopération numérique.

Les rapports post-Davos notent que la participation a été réduite de moitié et que l'absence de la Russie et de la Chine a rendu les discussions moins globales, et donc moins significatives.

Les critiques notent également que l'ambiance à Davos était « épouvantable », que des invités de haut niveau manquaient à l'appel et que le forum a laissé ses participants se demander si la mondialisation était morte.

Les critiques disent que Davos s'est conclu sans solutions définitives pour la guerre en Ukraine, les crises alimentaire et énergétique, et l'incertitude économique.

Dans le domaine du numérique, Davos a tenté d'envisager quelques solutions. Un certain nombre d'initiatives ont été lancées.

- L'initiative sur les investissements étrangers directs dans le domaine du numérique, lancée par le Forum économique mondial et l'Organisation de coopération numérique (DCO), offrira des informations uniques sur la manière de créer un écosystème numérique qui apporte la prospérité aux personnes, afin d'aider les gouvernements à mieux servir leurs citoyens et d'encourager les entreprises à se développer.
- Le Digital Inclusion Navigator aide les décideurs à trouver les meilleures pratiques et ressources pour favoriser l'inclusion numérique. La plateforme se concentre sur l'élargissement de l'accès aux technologies numériques et de leur utilisation, ainsi que sur le rôle des services numériques dans les soins de santé, les services financiers et l'éducation.
- Le réseau des pays phares, dirigé par le Programme des Nations unies pour le développement (PNUD) et un réseau de pays phares comprenant le Bahreïn, le Bangladesh et le Rwanda, est lancé pour accélérer l'inclusion numérique dans les secteurs de la santé, de l'éducation et de la finance sur le plan national.
- La promesse de cyber-résilience, défendue par le WEF et les entreprises de l'industrie pétrolière et gazière, décrit un engagement visant à renforcer la cyber-résilience dans l'ensemble de l'industrie en adoptant des cadres et des lignes directrices exploitables, en collaborant sur les défis communs de l'industrie et de la chaîne d'approvisionnement, et en partageant l'expérience apprise.
- Le WEF a annoncé le lancement d'un dialogue mondial sur la coopération numérique. Il reste à voir ce que cela signifie et comment cela s'alignera sur les initiatives de coopération numérique en cours aux niveau des Nations unies (nous pensons, par exemple, à l'élaboration du Pacte numérique mondial préconisé par le Secrétaire général des Nations unies dans son rapport « *Our Common Agenda* »).

Mises à jour des politiques de la Genève internationale

De nombreuses discussions politiques ont lieu chaque mois à Genève. Dans cet espace, nous vous informons de tout ce qui s'est passé au cours des dernières semaines. Pour d'autres comptes rendus d'événements, visitez la section « Événements passés » sur notre GIP Digital Watch Observatory.

2–22 mai 2022 | Semaine des réseaux et partenariats humanitaires (HNPW)

La conférence hybride HNPW a rassemblé des réseaux et des partenariats humanitaires pour aborder des questions humanitaires essentielles. Il s'agit de l'un des plus grands événements humanitaires de ce type, qui a rassemblé des participants des Nations unies, des ONG, des États membres, du secteur privé, de l'armée, du monde universitaire et d'autres organisations pour discuter des défis communs dans le domaine humanitaire.

10 mai 2022 | Décortiquer la réglementation européenne sur les marchés et services numériques

À la lumière du récent accord politique conclu entre le Parlement européen et les États membres de l'UE sur le paquet de mesures relatives aux services numériques (Digital Services Act – DSA), les panélistes ont discuté des défis économiques, éthiques et politiques liés au développement de grandes plateformes numériques et de services intermédiaires. Ils ont également analysé le travail législatif réalisé par les institutions européennes, et ont énuméré les défis liés à la mise en œuvre de la DSA et de la Digital Markets Act (DMA). Le webinaire a été organisé par la Représentation permanente de la France auprès de l'ONU à Genève, la Geneva Internet Platform (GIP) et la Délégation de l'Union européenne auprès de l'ONU à Genève.

22–28 mai 2022 | 75e Assemblée mondiale de la santé

Des représentants des États membres de l'Organisation mondiale de la santé se sont réunis à Genève pour discuter de la santé pour la paix et de la paix pour la santé. À la lumière de la pandémie de COVID-19, les participants ont échangé des idées sur la manière de renforcer la préparation de l'OMS et de ses États membres pour répondre aux urgences sanitaires.

27 mai – 11 juin 2022 | 110e session de la Conférence internationale du travail

Les États membres de l'Organisation internationale du travail (OIT) se réunissent pour discuter des conditions de travail en matière de sécurité et de santé au travail dans le cadre des principes et droits fondamentaux au travail de l'OIT. Les délégués entreprennent également la première discussion sur l'apprentissage en vue d'établir une nouvelle norme internationale du travail. Ils commenteront également le rapport « Travail décent et économie sociale et solidaire ». À cet égard, un document final devrait être adopté et sera soumis à la plénière de la Conférence pour adoption le 11 juin.

Ce qu'il faut surveiller : événements relatifs à la politique numérique mondiale en juin

Jetons un coup d'œil au calendrier mondial des politiques numériques. Voici ce qui se déroulera dans le monde entier. Pour plus d'événements, visitez la section Événements du Digital Watch Observatory.

6-10 JUIN
RightsCon2022
(en ligne)

La 11e édition de la conférence « RightsCon » sera organisée en ligne, car son organisateur, *Access Now*, estime que cela augmentera considérablement l'accessibilité et améliorera la représentation de toutes les parties concernées. Le programme comprend 18 catégories telles que l'IA, la politique en matière de contenu, la sécurité numérique pour les communautés, les cyber-normes mondiales, la vie privée et la surveillance, ainsi que l'accès à l'Internet, l'éducation et l'inclusion.

6–15 JUIN
Conférence mondiale du développement des télécommunications de l'UIT (CMDT-21)
(Kigali, Rwanda)

La Conférence mondiale de développement des télécommunications (CMDT-21) de l'Union internationale des télécommunications (UIT) se tiendra entre deux conférences plénipotentiaires. Conçue par le Bureau de développement des télécommunications (BDT) de l'UIT, elle a pour principal objectif d'examiner les sujets, les projets et les programmes relatifs au développement des télécommunications, et de définir les stratégies et les objectifs de développement des télécommunications/TIC. Le thème de l'événement est « Connecter les non-connectés pour atteindre le développement durable ». Alors qu'il reste dix ans pour atteindre les objectifs de développement durable (ODD), cet événement vise à accélérer les actions en vue de leur réalisation par le biais d'approches innovantes et de nouveaux modèles de collaboration pour la connectivité et les solutions numériques.

13–16 JUIN
ICANN74
(La Haye - Pays-Bas)

ICANN74 se tiendra sous la forme d'un forum politique prévu du 13 au 16 juin 2022. Composé de près de 100 sessions, le programme s'articulera autour de sujets tels que les procédures ultérieures des nouveaux domaines génériques de premier niveau (gTLD), l'acceptation universelle, le modèle multipartite de l'ICANN et les mises à jour des politiques générales des diverses organisations de soutien et comités consultatifs de l'ICANN.

20–22 JUIN
EuroDIG
(Trieste, Italie)

Le 15e dialogue européen sur la gouvernance de l'Internet (EuroDIG) abordera des sujets dans quatre domaines principaux : « Souveraineté numérique : L'Europe va-t-elle dans la bonne direction pour assurer la sécurité et l'ouverture de l'Internet ? » ; « Confrontation avec la réalité : Mettons-nous en œuvre des réglementations efficaces et établissons-nous les bonnes normes pour résoudre les problèmes de demain ? » ; « A venir – les organes de gouvernance existants peuvent-ils faire face aux défis des nouvelles technologies ? » ; « L'Internet en période de crise ». À travers ces domaines, la conférence répondra à la question posée lors du premier événement préparatoire d'EuroDIG : « Comment mettre en pratique les messages du FGI de Katowice ? » EuroDIG 2022 incluera également le « Dialogue des jeunes sur la gouvernance de l'Internet » (YOUthDIG). La GIP s'associera à nouveau à EuroDIG pour transmettre les messages et les rapports de l'événement, qui seront disponibles sur le *Digital Watch* Observatory.

26–28 JUIN
Sommet G7
(Alpes bavaroises, Allemagne)

Le sommet du G7 sera organisé sous la présidence de l'Allemagne sur le thème « Progresser vers un monde équitable ». La présidence allemande se concentre sur cinq domaines d'action : « une planète durable », « la stabilité et la transformation de l'économie », « des vies saines », « l'investissement dans un avenir meilleur » et « devenir plus fort ensemble ». Il s'agira notamment de promouvoir un engagement fort en faveur d'une numérisation inclusive.

A propos de ce numéro

A propos de ce numéro : Numéro 70 du bulletin *Digital Watch*, publié le 7 juin 2022 par la Geneva Internet Platform et la DiploFoundation, sous une licence CC BY-NC-ND 4.0 | Contributeurs : Andrijana Gavrilović (rédactrice), Kristina Hojstricova, Pavlina Ittelson, Arvin Kamberi, Marco Lotti, Anđelija Mijatović et Sorina Teleanu | Design : Diplo's CreativeLab |
Contact : digitalwatch@diplomacy.edu

Sur la couverture :

Le marché des crypto-monnaies en danger ? Credit: Vladimir Veljasević

La Geneva Internet Platform est une initiative de :

GENEVA INTERNET PLATFORM digwatch

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

REPUBLIQUE ET CANTON DE GENEVE

DiPLO
www.diplomacy.edu