Brunngasse 36
CH-3011 Bern
www.ta-swiss.ch

«Update, zwischen Sicherheit, Souveränität und Nachhaltigkeit»

Ausschreibungs-Unterlagen zur Studie

Termin für die Eingabe von Projektskizzen	**02.11.2023**
Termin für die Eingabe von Projektofferten:	**05.02.2024**

mitglied der akademien der wissenschaften schweiz

Stiftung für Technologiefolgen-Abschätzung
Fondation pour l'évaluation des choix technologiques
Fondazione per la valutazione delle scelte tecnologiche
Foundation for Technology Assessment

1. Themenbeschrieb (auf Französisch)

Die einen loben sie über den grünen Klee, die anderen lehnen sie ab: Für die Sicherheit unserer Daten und für das verlässliche Funktionieren der Informatiktools sind Updates unabdingbar. Sie ermöglichen es einerseits, dass sich die Tools weiterentwickeln und somit attraktiv bleiben. Andererseits bergen sie auch Risiken: Unter Umständen führen Software-Aktualisierungen zu Fehlfunktionen oder können die Kapazität eines Geräts überfordern bzw. dieses gar unbrauchbar machen. Angesichts der zunehmend häufigen Updates und der Vielschichtigkeit ihrer Folgen sind Benutzerinnen und Benutzer gezwungen, Entscheidungen zu fällen, ohne sich über deren Auswirkungen vollständig im Klaren zu sein. Je nachdem, wie wichtig ein Gerät für die Arbeit oder die Gestaltung des Alltags ist, können Updates private Nutzerinnen und Nutzer, Firmen oder auch den Staat in unerwünschte Abhängigkeiten führen.

Ubiquité

L'informatique ubiquitaire est la troisième ère de l'informatique moderne[1]. Elle succède à l'ère des ordinateurs personnels et celle des ordinateurs centraux. Cette nouvelle ère informatique se caractérise par une explosion d'outils informatiques connectés à internet et gérés par un logiciel. Ils sont présents à tout moment et dans tous les domaines de nos vies que ce soit dans la sphère privée ou professionnelle. Tous ces appareils interconnectés faisant partie de l'internet des objets, mais aussi les applications, les interfaces et les jeux de données évoluent grâce à des mises à jour afin de s'adapter aux changements constants. Nous sommes parfois invités à effectuer des mises à jour pour certains des produits que nous possédons, mais pour d'autres ses mises à jour se font automatiquement de manière invisible et en continu. Les mises à jour sont donc incontournables. Même si à titre privé une personne souhaiterait se déconnecter totalement d'internet, les infrastructures qu'elle utilise eau, électricité, sont-elles gérées par des systèmes informatiques qui doivent être eux aussi régulièrement mis à jour.

Complexité

Lorsqu'un utilisateur se retrouve face à une demande de mise à jour, il s'avère souvent difficile de comprendre en quoi elle consiste exactement. Quel est son but et à quel point est-elle nécessaire ou non ? Quelles sont les implications et les interdépendances et surtout comment va se comporter l'outil informatique à la suite d'une mise à jour ? On ne peut pas exiger de chaque usager qu'il devienne un expert dans le domaine. Pourtant un degré minimum de connaissances est requis. Dans certaines circonstances nous acceptons d'utiliser des dispositifs dont nous ne comprenons pas entièrement le fonctionnement, mais dans le cas des mises à jour, nous devons parfois prendre une décision et agir. Chaque mise à jour est une remise en question, il faut donc à chaque fois refaire une évaluation de la situation.

[1] John Krumm, Ubiquitous Computing Fundamentals, CRC Press - 2009

Evolutivité

Le changement constant et extrêmement rapide des produits informatiques peut aussi rendre difficiles certaines obligations de contrôle et de suivi de l'Etat. Par exemple, lorsque l'autorisation d'une administration est requise pour la vente d'un produit, celle-ci se prononce sur une version du produit qui sera ultérieurement modifiée par une mise à jour. Par ailleurs, la fréquence des mises à jour complique l'éventuelle réglementation de produits numériques. Ainsi, dans une réponse à une interpellation parlementaire du conseiller aux Etats Beat Vonlanthen (Le Centre) au sujet du marché suisse, le Conseil fédéral considère que les mises à jour constituent un obstacle à la certification ou l'élaboration de normes d'évaluation de produits électroniques :

« [...] la vie de ces produits [numériques] est jalonnée de nombreuses mises à jour, raison pour laquelle un système statique de certifications de produits ne déploierait que des effets limités. Dans ce contexte dynamique, il faut partir du principe que les acteurs du marché sont mieux placés que le Conseil fédéral pour connaître les exigences auxquelles doivent satisfaire les produits. » (18.3511).

Malgré la difficulté à suivre le rythme des mises à jour, on peut se demander s'il est adéquat de laisser quelques grands acteurs de la Tech fixer les normes.

La rapidité des changements est telle qu'aujourd'hui beaucoup d'outils ne fonctionnent pas avec la dernière version accessible. C'est le cas des ordinateurs personnels où l'utilisateur ne fait sciemment pas toujours les mises à jour dans l'immédiat, mais aussi dans le domaine de l'IoT. Une analyse faite en février 2023 révèle que moins de 3% des IoT dispersés dans le monde emploient le dernier *firmware* disponible.[2] Cette évolutivité est donc difficile à gérer tant pour l'amateur que pour l'ingénieur spécialiste de la question. L'opacité de tous ces changements est accentuée par le fait que certaines mises à jour sont automatiques et quasi invisibles pour l'usager. Celui-ci n'a parfois même pas accès à la liste des mises à jour effectuées. Le lien de confiance avec le producteur d'outils informatiques et avec le fournisseur de mises à jour est d'autant plus important. La relation ne s'arrête donc plus au moment de la vente. Comme les dispositifs informatiques se modifient en continu, ils s'accompagnent de plus en plus d'un service. Le modèle d'abonnements, de *Software as a service* (SaaS) ou - comme le dénomme Tien Tzuole CEO de Zuora - la „subscription economy" se généralisent. Ces modèles ne se limitent plus au *software*, méthode courante chez des fournisseurs de logiciels tels que Microsoft ou Adobe, mais s'appliquent également au *hardware*, Apple l'envisagerait pour ses iPhones [3]. La pratique s'étend d'ailleurs au domaine automobile. BMW propose des sièges chauffants activables à distance avec la technologie over the air (OTA) après avoir payé un forfait. L'entreprise s'est du

[2] F. Ebbers, "A Large-Scale Analysis of IoT Firmware Version Distribution in the Wild," in IEEE Transactions on Software Engineering, vol. 49, no. 2, pp. 816-830, 1 Feb. 2023, doi: 10.1109/TSE.2022.3163969.
[3] « Apple Is Working on a Hardware Subscription Service for iPhones » (Bloomberg 2022, https://www.bloomberg.com/news/articles/2022-03-24/apple-is-working-on-a-hardware-subscription-service-for-iphones?sref=9hGJlFio).

reste déjà attiré des critiques (« on paie à double »), mais aussi l'attention de hackers qui sont parvenus à les détourner.[4]

A travers des abonnements permettant d'avoir en tout temps la meilleure version d'un outil informatique, l'utilisateur a la garantie d'être toujours à jour, mais il développe de même une dépendance très forte à l'entreprise qui fournit l'appareil ou l'accès au logiciel. De plus lorsqu'un accord est donné pour une certaine fonction ou un certain service et que celui-ci change suite à une mise à jour, il n'est pas aisé de déterminer à partir de quel niveau de modification on estime que la fonction ou le service ne correspond plus à l'accord initial.

Souveraineté

La personne ou l'entité qui a réellement besoin d'un programme ou d'un appareil est plus ou moins obligée d'accepter les mises à jour pour continuer à l'utiliser dans de bonnes conditions, sous peine de subir de gros coûts de sortie. Cette problématique reste présente qu'on ait acheté un logiciel ou souscrit à un abonnement. Pour un état, ces dépendances peuvent aller à l'encontre de sa souveraineté et plus spécifiquement sa capacité à agir dans le cyberespace. Ce problème a notamment été soulevé dans une interpellation parlementaire portant sur la souveraineté numérique, face à l'usage de Microsoft par l'Administration fédérale.[5] L'utilisateur d'un outil soumis à des mises à jour est non seulement dépendant des choix stratégiques de l'entreprise par rapport aux mises à jour, mais aussi du destin de celle-ci. En effet si elle fait faillite ou est rachetée par un concurrent l'usage de l'outil peut être compromis. Certains misent sur l'open source afin de minimiser cette dépendance et garantir une certaine pérennité de l'outil informatique. Mais beaucoup préfèrent le sentiment de confiance (relative) fournie par une grande entreprise qui aura les moyens de maintenir ses produits à jour[6]. Un utilisateur se retrouve donc rapidement tributaire des choix du fournisseur et sa marge de manœuvre limitée une fois qu'il opte pour un produit informatique. De plus l'usager devra souvent adapter son fonctionnement à l'outil qu'il aura choisi, ce qui augmente encore sa dépendance à cet outil et à son prestataire de services. Et cela même si avec les mises à jour successives le produit évolue dans une direction qui ne convient plus aux besoins de l'utilisateur.

---

[4] Voir « Attention, BMW fera des émules avec son abonnement pour sièges chauffants… » (Le Temps, mai 2022, https://www.letemps.ch/economie/attention-bmw-fera-emules-abonnement-sieges-chauffants) ou « Sitzheizung for free: Hacker untergraben Abo-Modell von BMW » (Br24, juillet 2022, https://www.br.de/nachrichten/netzwelt/sitzheizung-for-free-hacker-untergraben-abo-modell-von-bmw,TCDjrVQ).

[5] 17.3783 : « Beispielsweise gab Microsoft Ende 2014 bekannt, dass keine Sicherheits-Updates mehr für Windows XP geliefert werden. Somit musste beispielsweise die britische Regierung für über 7 Millionen Franken einen Vertrag mit Microsoft abschliessen, dass diese weiterhin Fehler in ihrer Software reparieren. »

[6] recommandation donnée aux PME dans l'article du journal Bilan https://www.bilan.ch/story/a-lheure-du-tout-numerique-les-pme-doivent-faire-les-bons-choix-strategiques-566226914295

Sécurité

La gestion des mises à jour est donc complexe à plusieurs niveaux, pourtant elles sont essentielles à la protection contre la cybercriminalité. 60% des cyberattaques seraient dues à des logiciels non mis à jour[7]. Le centre national pour la cybersécurité (NCSC) conseille donc fortement d'avoir tous ses appareils avec les dernières mises à jour[8]. Or une mise à jour même mineur peut aussi apporter une faille au système et le rendre ainsi vulnérable. Certains techniciens conseillent d'ailleurs de ne pas les faire tout de suite, car les répercussions d'une mise à jour inadaptée peuvent être plus graves que les éventuels dangers de cyberattaque[9]. Les entités qui le peuvent s'équipent d'un service IT qui gère les risques ainsi que la qualité et la compatibilité des mises à jour. Mais comment aider les utilisateurs qui n'ont pas les moyens d'avoir une équipe d'experts ? Laisser chacun choisir son niveau de vulnérabilité et en subir individuellement les conséquences n'est pas une solution, puisqu'un équipement vulnérable peut être une porte d'entrée pour tout un système et donc compromettre plusieurs autres appareils. Par analogie on ne laisse pas un automobiliste choisir lui-même les critères de sécurité que son véhicule doit remplir. Comme il circule sur la voie publique, son automobile doit répondre à des normes et passer des inspections régulières. La façon de conduire est elle aussi fortement réglementée. Cela nous parait aujourd'hui une évidence, mais ce n'a pas toujours été le cas[10]. Peut-être que dans quelques années il y aura des réglementations similaires pour naviguer dans le cyberespace tant pour les appareils que pour les utilisateurs.

Responsabilité(s)

Utiliser des outils informatiques connectés est donc un acte qui peut avoir des répercussions sur autrui. Cette responsabilité envers la sécurité des autres peut être sous-estimée par beaucoup. En refusant des mises à jour par crainte des conséquences non prévisibles sur son système, une entreprise prend le risque de mettre en péril les données de ses clients en se rendant vulnérable à des cyberattaques [11]. Avec le développement du home office et du travail en ligne cette gestion se complexifie d'autant plus, surtout pour les PME [12]. En cas de litiges il n'est pas aisé de savoir quelles sont les différentes dispositions légales et qui doit assumer les éventuels dommages. Les questions de responsabilité se posent aussi pour tout objet géré par un logiciel. Que se passerait-il si une voiture entre en collision avec un piéton et que l'assurance du conducteur estime que l'accident aurait été évité grâce à la dernière mise à jour qui n'a pas été installée. Et si

---

[7] Selon l'étude Costs and Consequences of Gaps in Vulnerability Response de l' Institut Ponemon aux USA, cité par Institut national de test pour la cybersécurité.
[8] Voir sur le site du NCSC https://www.ncsc.admin.ch/ncsc/fr/home/aktuell/im-fokus/ks-update.html et plus spécifiquement la campagne S-U-P-E-R https://www.s-u-p-e-r.ch/fr/home/
[9] Emission RTS - On en parle, épisode du 18.01.2021 « Les dangers des mises à jour système » https://pages.rts.ch/la-1ere/programmes/on-en-parle/18-01-2021
[10] Le permis de conduire est obligatoire au plan national depuis 1932. Les premières directives au niveau cantonal remontent à 1904. informations issues des archives OFROU.
[11] Voir «Why don't big companies keep their computer systems up-to-date? » (*The Conversation*, 2017: https://theconversation.com/why-dont-big-companies-keep-their-computer-systems-up-to-date-84250).
[12] https://www.kmu.admin.ch/kmu/fr/home/actuel/news/2021/les-pme-sont-en-retard-en-matiere-de-securite-digitale.html

au contraire la dernière mise à jour a un bug et rend le système de reconnaissance des piétons moins efficace. Déterminer les responsabilités devient de plus en plus complexe et porter plainte encore plus puisque les entités sont multiples et souvent internationales.

Durabilité

Pour les entreprises fabriquant des appareils et logiciels, il existe dans certains pays des obligations de fournir des mises à jour.[13] Pour d'autres, la motivation vient de la nécessité d'assurer leur compétitive sur le marché et permettre à leur produit d'être plus longtemps fonctionnels et attractifs. Or les mises à jour ne sont pas toujours appréciées et les dysfonctionnements ou ralentissements induits par certaines évoquent une pression à l'achat de nouveaux produits, voire une stratégie d'obsolescence programmée.[14] Il peut même arriver que des mises à jour de système endommagent définitivement l'appareil à l'exemple de la mise à jour OS Big Sur de Apple en novembre 2020.[15] Ces problèmes ont été brièvement discutés au Parlement dans le cadre de l'initiative parlementaire 18.459 « Inclure tous les éléments faisant partie intégrante de l'objet dans la garantie pour les défauts » (déposée par le conseiller national Samuel Bendahan, PS). Il semble y avoir eu un consensus sur le point suivant : « l'idée que l'on puisse, par les mises à jour, vous saboter votre appareil scandalise à juste titre » (propos du conseiller national Yves Nidegger (UDC), pour la commission).

Inversement, dans d'autres contextes, c'est la fin des mises à jour d'un produit qui est décriée, car cela nous pousserait à continuellement acheter de nouveaux produits, sans égard pour l'écologie[16]. Ainsi, il est conseillé de se renseigner avant de se procurer un produit, sur le nombre de mises à jour garanties, notamment pour les smartphones[17]. Placer ce critère en avant devrait éviter d'acquérir un appareil a priori attractif, mais qui sera précocement obsolète. Pourtant ces informations ne sont pas clairement communiquées, ce qui complique la prise de décision du consommateur.

---

[13] Voir par exemple le récent changement de loi en Allemagne : « Bundestag beschließt Update-Pflicht » (*Spiegel*, juin 2021 : https://www.spiegel.de/netzwelt/netzpolitik/bundestag-beschliesst-update-pflicht-a-f96477af-4917-417d-965c-8a2e1799b343).

[14] Voir « Are our phones really designed to slow down over time? Experts look at the evidence » (*The Conversation*, 2021, https://theconversation.com/are-our-phones-really-designed-to-slow-down-over-time-experts-look-at-the-evidence-170962).

[15] Voir https://www.srf.ch/news/panorama/update-panne-vorsicht-vor-neustem-update-aeltere-mac-computer-koennen-abstuerzen ou en français Emission RTS - On en parle, épisode du 18.01.2021 « Les dangers des mises à jour système » https://pages.rts.ch/la-1ere/programmes/on-en-parle/18-01-2021

[16] Voir « Best Before date policy brief: Device sustainability through long-term software support » (Privacy International, 2021, https://privacyinternational.org/advocacy/4636/best-date-policy-brief-device-sustainability-through-long-term-software-support) ou l'article du Spiegel cité plus haut.

[17] Emission RTS - On en parle, épisode du 9.11.2022 "Les mises à jour des smartphones: un critère d'achat important » interview de Léa Nuel, hackeuse éthique chez SCRT https://pages.rts.ch/la-1ere/programmes/on-en-parle/09-11-2022

2. Fragen von Interesse für die TA-SWISS-Studie

Technische Fragen

- Wie lassen sich bei Aktualisierungen kleinere Korrekturen von grösseren Modifikationen unterscheiden, und wie kann man diesen Unterschied kommunizieren? Welche Freiheit ist den Benutzenden bei der Wahl der Updates einzuräumen, ohne dass es zu unüberschaubaren Zuständen kommt?
- Die wechselseitigen Abhängigkeiten bei Aktualisierungen sind komplex; wie viel Transparenz muss oder kann dem Nutzer geboten werden? Wie ist es möglich, im Hintergrund automatisiert ablaufende Updates trotzdem nachzuverfolgen und einen Rechenschaftsbericht anzufordern?
- Die meisten IoT-Geräte funktionieren mit dem neuesten Update nicht. Wie lässt sich die Ausbau- und Erneuerungsfähigkeit von IT-Tools verbessern?

Wirtschaftliche Fragen

- Werden Software in einer Cloud (SaaS) und das Abonnementmodell (subscription economy) zur Norm? Welches sind die Vor- und Nachteile für die Nutzenden? Was hat der Anbieter davon? Steuern wir auf das Ende des Eigentums zu?
- Viele setzen ihre Hoffnung auf Open Source, um die Abhängigkeit von einem Anbieter zu minimieren. Wie finanziert sich Open Source-Entwicklung?
- Die Handhabung von IT-Tools und deren Aktualisierungen wird immer komplexer. Wie reagieren IT-Abteilungen auf die Anforderungen? Welche Möglichkeiten bieten sich?

Fragen bezüglich der Umwelt

- Kann man Anbieter von IT-Geräten dazu verpflichten, für ihre Produkte eine Mindestdauer von Updates zu garantieren? Wie geht man damit um, wenn der Hersteller des Geräts und der Anbieter der Software nicht identisch sind?
- Würde die Möglichkeit der offline-Nutzung dazu führen, dass Geräte länger genutzt werden können, die zwar noch funktionieren, aber keine neuen Updates mehr verkraften?
- Wie lässt sich feststellen, ob ein Gerät vom frühzeitigen Verschleiss (programmierte Obsoleszenz) betroffen sein wird?
- Was müsste unternommen werden, damit die stetige Verbesserung eines Produkts zugleich als Chance zur Reduzierung von Computerabfällen genutzt werden könnte?

Rechtliche (schweizspezifische) Fragen

- Wie geht man mit Inkompatibilitäten bei Updates um, die davon herrühren, dass Hardware und Software oft nicht vom gleichen Unternehmen stammen? Wer trägt die Verantwortung, wenn die Software die Hardware beschädigt?
- In Anbetracht des Umstands, dass es für Hardware eine Garantie gibt, für Software aber nicht, welche Konflikte können daraus entstehen? Wie können diese begleitet und reguliert werden?

- Welche Regelungen gibt es derzeit für Störfälle, die sich durch die Installation des aktuellsten Updates hätten vermeiden lassen? Oder umgekehrt für Vorfälle, die durch ein fehlerhaftes Update ausgelöst wurden?
- Die Kundschaft unterschreibt einen fest vereinbarten Vertrag, aber das verwendete Produkt verändert sich - wie geht man mit diesem Widerspruch um? Wie verhält es sich mit kostenlos online manipulierten Werkzeugen, bei denen der Nutzer seine Zustimmung gibt? Steht fest, was genau diese Zustimmung umfasst und bis wohin sie reicht?

Gesellschaftliche Fragen

- Wie nehmen die Menschen Aktualisierungen wahr, und welche Beziehung haben sie zu dieser Aktion? Sind sie sich über alle Auswirkungen im Klaren?
- Welches Mass an Wissen darf man vernünftigerweise von jeder Person erwarten, die Computerwerkzeuge benutzt?
- Welche Arten von Verantwortlichkeiten kann von den Nutzenden verlangt werden? Besteht eine Pflicht zur Wachsamkeit? Sollten bestimmte Verhaltensregeln eingeführt werden, die einzuhalten sind? Wenn ja, welche?
- Wie verändern die sich ständig weiterentwickelnden IT-Tools die Arbeitsweisen derjenigen, die sie nutzen? Wie beeinflussen sie die alltäglichen Gewohnheiten?
- Könnten Updates die digitale Kluft in der Gesellschaft vertiefen, und wenn ja, aus welchem Grund? Welche Massnahmen könnten ergriffen werden, um dies zu verhindern?
- Welche Trends zeichnen sich in der Bevölkerung angesichts des dynamischen und kontinuierlichen Wandels ab? Macht sich eher Ermüdung oder Begeisterung breit?
- Wie können wir abschätzen, ob unsere starke Vernetzung mit IT-Tools uns abhängiger und verletzlicher macht?

Politische Fragen

- Wenn IT-Tools miteinander verbunden sind, wirken Updates nicht nur auf ein einzelnes Gerät, sondern auf ein ganzes System zurück. Wäre es vertretbar, Updates zu erzwingen? Welches Gleichgewicht gilt es zwischen der Sicherheit aller Nutzenden und den Entscheidungen der Individuen zu finden? Welche Rolle kommt dem Staat zu? Muss er das Ganze koordinieren?
- Derzeit diktieren die grossen Tech-Akteure die Standards im IT-Sektor. Ist das problematisch? Welche rechtlichen Rahmenbedingungen kann der Staat vorgeben?
- Ist es angesichts der Abhängigkeit vieler Nutzenden von den Tech-Giganten denkbar, dass es im IT-Bereich Unternehmen gibt, die «too big to fail» sind?
- Wie sollte der Staat den Teil der Gesellschaft begleiten, der sich entscheidet, nicht mitzuhalten, nicht «aktualisiert» zu sein? Wird es noch vertretbar oder gar möglich sein, informationstechnisch nicht auf dem neusten Stand zu sein?
- Wie geht die Regierung mit IT-Dienstleistungen oder IT-Komponenten um, die in die Hände kriegsführender Länder geraten könnten?
- Wie gelingt es einem Staat, im Cyberspace seine Souveränität zu wahren?

3. Angaben zum Inhalt und zur Durchführung der Studie

3.1. Inhalt der Studie

Die **interdisziplinäre Studie** soll die **Chancen und Risiken der Updates** von Informatiktools ausloten, insbesondere im Hinblick auf die **Cybersicherheit**, die **Souveränität**, die **Nachhaltigkeit** sowie auf ihre allgemeinen Auswirkungen auf die Gesellschaft und auf unsere **Lebensstile**.

Es sollen die **technischen, rechtlichen, wirtschaftlichen, ökologischen, gesellschaftlichen und politischen Implikationen** von Updates untersucht werden.

Da Updates jederzeit die meisten unserer täglichen Aktivitäten beeinflussen, gilt es, ein breites Untersuchungsfeld abzudecken. In den Blick zu nehmen sind die Infrastrukturen der Informatik als solche, die **Clouds** wie auch verschiedene **Software-Typen**, das **Internet der Dinge** (IoT) und ebenso die **künstliche Intelligenz** (KI). Denn all diese Bereiche benötigen Updates und sind somit in der Studie zu behandeln.

Vielfältig sind auch die von Updates betroffenen Nutzergruppen. Die Studie wird sich daher sowohl mit der **Bevölkerung** befassen als auch mit **wirtschaftlichen Kreisen**, **den Betreibern kritischer Infrastrukturen** und den **Behörden auf Ebene Bund, Kantone und Gemeinden**. All diese Gruppen sind mit unterschiedlichen Herausforderungen konfrontiert. Die Wechselwirkungen der verschiedenen Software und ihre Folgen für deren Verwendung gilt es herauszuarbeiten, und zwar spezifisch für jede Benutzergruppe.

Angesichts immer häufiger anfallender Updates sind mittlerweile Geschäftsmodelle mit Abonnements gang und gäbe: Um mit der steten Weiterentwicklung der Technik Schritt zu halten, verkaufen Konzerne keine Geräte, Software oder Daten mehr, sondern eine Garantie für den fortlaufenden Leistungsbezug. Mithin ist in der Studie das Phänomen der **«subscription economy»** zu berücksichtigen.

Allerdings ist nicht alles veränderlich und flüchtig. Der Kontrast zwischen der **Dynamik digitaler Produkte** und dem relativ **starren gesetzlichen Rahmen** wirft Probleme auf. Weil sich die Funktionalitäten und Leistungen eines Informatiktools ständig verändern, kann es auf vertraglicher Ebene zu Unstimmigkeiten mit den ursprünglichen Vereinbarungen kommen, die für eine bestimmte Version des Produkts zu einem bestimmten Zeitpunkt eingegangen wurden. Diese Diskrepanz ist aus rechtlichen und ethischen Gesichtspunkten zu untersuchen.

Abgesehen von der Analyse der Vertragsbeziehung, die mit dem Abschluss eines Abonnements oder mit der Zustimmung zu den Updates entsteht, soll die Studie auch die **Abhängigkeit** der Nutzenden zu den Leistungserbringern ausleuchten. Das einseitige Machtverhältnis kann sich für die verschiedenen Nutzertypen als riskant erweisen und die **Souveränität** eines Staates infrage stellen.

Dennoch sind die Updates für die **Cybersicherheit** unerlässlich. Kommt hinzu, dass nicht nur die individuelle Ausstattung geschützt werden muss, sondern ein ganzes System. Diesen Verbund gilt

es zu analysieren, wie auch den Handlungsspielraum, der allen Nutzenden für **Vorsorgemassnahmen** zum Schutz ihrer Informatikausstattung gelassen wird.

Mit Blick auf Störfälle sind Updates mitnichten harmlos. Werden sie nicht installiert, drohen **Schwachstellen** oder gar völliger Kontrollverlust. Doch auch fehlerhafte Aktualisierungen können problematisch sein. Die **Verantwortlichkeit** aller Beteiligten steht keineswegs fest und es gilt diese, wie auch allfällige rechtliche Lücken, auszuleuchten.

Auch Aspekte der **Nachhaltigkeit** sind wichtig und müssen behandelt werden. Dies wird oft vernachlässigt, da Sicherheitsfragen meistens im Vordergrund stehen. Es wird in der Studie einerseits darum gehen zu ermitteln, inwiefern **die Leistung eines Produkts** dank Updates verbessert wird und damit seine **Attraktivität und Lebensdauer** verlängert werden können. Andererseits gilt es zu analysieren, ob zu häufige Updates das Risiko eines vorzeitigen Verschleisses von Geräten – ihre **Obsoleszenz** – erhöhen.

Um ein Gleichgewicht zwischen Souveränität, Sicherheit und Nachhaltigkeit zu finden, wird es wichtig sein, die verschiedenen Faktoren zu verstehen und auszuwerten, die jede Nutzergruppe dazu bringen, Updates zu akzeptieren oder abzulehnen. Daher sind **Befragungen** oder der Einsatz **partizipativer Ansätz**e in Betracht zu ziehen.

Abschliessend ist eine **Gesamtbeurteilung** vorzunehmen, und beruhend darauf sollen **Schlussfolgerungen** gezogen und wenn möglich **Empfehlungen** zum Umgang mit der Problematik formuliert werden, die an Entscheidungstragende, insbesondere an Politikerinnen und Politiker gerichtet sind.

3.2. Ablauf, Termine und Einreichungen

Einreichen von Projektskizzen

Die Ausschreibung erfolgt in einem zweistufigen Verfahren. In einem ersten Schritt sollen Projektskizzen abgegeben werden. Dabei sind zwei Dokumente einzureichen:

- Das Bewerbungsformular mit der geplanten Zusammensetzung des Forschungsteams und einer Zusammenfassung der wichtigsten geplanten Schwerpunkte. (Das Formular kann unter folgender Adresse heruntergeladen werden: https://www.ta-swiss.ch/updates)
- Eine Beschreibung, die den Inhalt der vorgeschlagenen Studie und den geplanten Ansatz beinhaltet:
    - Vorgesehener Inhalt der Studie: Schwerpunkte, Fragestellungen (1 Seite)
    - Geplantes Vorgehen und Forschungsmethoden (max. 2 Seiten)

Die Projektskizzen sind **bis spätestens am 2. November 2023** auf elektronischem Weg einzureichen (als pdf-Datei) an info@ta-swiss.ch.

Der Entscheid, welche Projektteams für eine weitere Bearbeitung eingeladen werden, wird voraussichtlich **Mitte Dezember 2023** fallen.

Einreichen einer ausführlichen Offerte

Auf Basis der eingereichten Projektskizzen werden in einem zweiten Schritt ca. drei Teams für eine weitere Bearbeitung eingeladen. Die ausgewählten Forschungsgruppen erhalten **Mitte Dezember 2023** Rückmeldungen zu ihren Eingaben und werden aufgefordert, **bis zum 5. Februar 2024** eine ausführliche Offerte einzureichen. In dieser zweiten Phase sind die «Richtlinien für die Eingabe von Projektofferten» gemäss Punkt vier der detaillierten Ausschreibungs-Unterlagen zu berücksichtigen.

3.3. Durchführung der Studie

Die Geschäftsstelle der Stiftung TA-SWISS wird eine Gruppe von Fachpersonen (Begleitgruppe) einsetzen, in welcher Personen vertreten sind, die sich mit unterschiedlichen Aspekten der Thematik befassen. Die zur Ausführung genehmigte Offerte wird vor Beginn der Projektarbeit von der auftragnehmenden Gruppe in der Begleitgruppe vorgestellt; bei der Diskussion des Projektvorschlags können die Begleitgruppe und die Geschäftsstelle Einfluss nehmen auf die Prioritäten und die Vorgehensweise. Die auftragnehmende Gruppe wird im weiteren Verlauf des Projekts drei- bis fünfmal Arbeitspapiere bzw. Zwischenberichte z.Hd. der Begleitgruppe und der Geschäftsstelle vorlegen. Diese dienen als Diskussionsgrundlage; die Durchführung der jeweils nächsten Arbeitsschritte erfolgt gemäss Absprache mit der Begleitgruppe bzw. der Geschäftsstelle.

3.4. Budget und zeitlicher Rahmen der Studie

- Budgetrahmen: CHF 100’000.- bis 160'000.-
- Projektbeginn: Juni 2023 (nach Absprache evtl. später)
- Projektdauer: ca. 12 bis 15 Monate

In diesem Budgetrahmen ist die Mehrwertsteuer eingeschlossen; es obliegt dabei der auftragnehmenden Projektgruppe abzuklären, ob sie mehrwertsteuerpflichtig ist.

3.5. Übrige Bestimmungen

- TA-SWISS untersteht nicht dem öffentlichen Beschaffungsrecht. Dies bedeutet, dass es gegen Entscheide hinsichtlich Annahme oder Ablehnung eingereichter Projektskizzen und -offerten kein ordentliches Rechtsmittel gibt.
- Es wird keine Korrespondenz zum Stand von eigereichten Projektskizzen und -offerten geführt.
- Potentielle Vertragspartnerinnen bzw. Vertragspartner haben kein Anrecht auf eine Entschädigung für deren Aufwand bei der Ausarbeitung von Projektskizzen und -offerten.
- Im Weiteren gelten bei Auftragserteilung die im *Vertrag* zwischen TA-SWISS und den Vertragspartnern aufgeführten Konditionen sowie die dem Vertrag beigefügten *Richtlinien für Begleitgruppen von TA-SWISS Studien.*

4. Richtlinien für die Eingabe von Projektofferten

Wir bitten Sie, bei der Formulierung Ihrer Projektofferte gemäss folgendem Aufbau-Raster vorzugehen (die unter den einzelnen Rubriken aufgezählten Angaben sind als **Beispiele** zu verstehen und brauchen daher nicht «im Wortlaut» berücksichtigt zu werden):

1. Ausgangslage und Begründung – Analyse der gegenwärtigen Situation

- Warum ist eine TA-Studie zum vorgeschlagenen Thema sinnvoll?
- Nationale und internationale Bedeutung der Thematik
- Technologische, wirtschaftliche, politische, gesellschaftliche Bedeutung
- Bisherige Forschungserkenntnisse, unter besonderer Berücksichtigung der für die Technikfolgen-Abschätzung relevanter Aspekte
- Zu erwartende Entwicklungen im vorgeschlagenen Themenfeld

2. Problemstellung

- Fragen, die es zu beantworten gilt
- Zielsetzung des Projektes bzw. der Studie
- Welche neuen Ergebnisse/Betrachtungsweisen bringt das vorgeschlagene Projekt?

3. Projektstruktur und Projektabgrenzung

- Zielgruppen, auf welche das Projekt fokussiert
- Allenfalls: Aufteilung in Haupt- und Teilprojekte
- Schon bestehende oder geplante Vernetzungen mit anderen Projekten, die ähnliche Fragestellungen behandeln (nationale und internationale Kontakte)

4. Methodik

- Methodische Ansätze, die zur Bearbeitung der Thematik in Frage kommen (eventuell Ausarbeitung von Varianten)
- Bewertung der Methoden; sind sie im Hinblick auf die Fragestellung angemessen? Begründeter Methodenvorschlag
- Beschreibung des empirischen Vorgehens
- Vorgesehene partizipative Methoden
- Art und Weise, wie der Interdisziplinarität bei der Erarbeitung der Studie Rechnung getragen wird

5. Projektkoordination

- Personelle Betreuung des Projektes; Projektleiter/-in, Mitarbeitende(r)
- Expertengruppen
- Wichtige Kontaktpersonen und Institutionen (mögliche Kooperations-Partner, s. auch unter 3)

6. Vorleistungen

- Liste der Arbeiten der Personen im Projektteam im Bereich der zu untersuchenden Thematik

7. Aktionsplan

- Zeitplan: Bis wann werden welche Arbeiten geleistet? Wer ist dafür zuständig?

8. Budget

- Detaillierter Finanzplan; Abschätzen des Mittelbedarfs für die unter Punkt 7 ausgewiesenen Einzelschritte

9. Umsetzung der Resultate

- Wie können die Ergebnisse der breiten Öffentlichkeit bekannt gemacht werden?
- Wie sind allenfalls ausgewählte Zielgruppen zu erreichen?
- Mit welchem zusätzlichen Finanzaufwand ist für die Umsetzung zu rechnen?