SIMPÓSIO INTERNACIONAL DE ARQUIVOS

Arquivo, documento e informação em cenários híbridos.

5 A 13 DE DEZEMBRO DE 2020

CONFIANDO NOS DOCUMENTOS ARQUIVÍSTICOS EM UM AMBIENTE EM REDE

Luciana Duranti
Diretora do Projeto InterPARES
University of British Columbia

EUGENIO OCCORSIO, ROMA

La Luiss Business School adotta per prima in Italia la tecnologia di ultima generazione: tutti i titoli e le competenze acquisite verranno riportati in un "registro" ipercontrollato e immodificabile accessibile sul web in tutto il mondo

Il caso più clamoroso è anche il più paradossale: Marilee Jones era la *dean of admissions*, ovvero la preside dello speciale istituto presso il Mit che vagliava le domande di ammissione. Bene: nel 2007 l'impietoso *investigative team* del Boston Globe svelò che aveva fabbricato il suo *curriculum* al momento dell'assunzione nel 1979 inserendovi ben tre lauree fasulle: dell'Union College, del Rensselaer Polytechnic Institute e dell'Albany Medical College. Ammise tutto e fu licenziata. Ma non è certo l'unica storia del genere: in ogni angolo del mondo il vizio di falsificare i titoli di studio è diffusissimo. La Germania è particolarmente severa: perfino Ursula von der Leyen nel 2015 fu accusata non di aver inventato la laurea ma di aver copiato la tesi senza citare le fonti. Fu creata una commissione di esperti indipendenti e in qualche modo se la cavò: non altrettanto bene era andata negli anni precedenti a due ministri del governo Merkel, Karl-Theodor zu Guttemberg e Annette Schavan (ministra dell'Istruzione), costretti alle dimissioni così come nel 2016 la deputata socialdemocratica Petra Hinz che non solo non era laureata come sosteneva ma non aveva neanche conseguito la licenza liceale.

Paolo Boccardelli direttore Luiss Business School

Giuseppe Perrone capo della sede EY di Roma

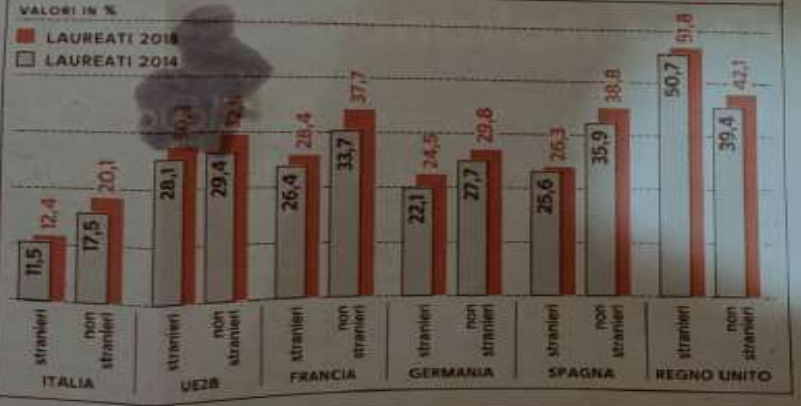
85%
LE "BUFALE"
Quota di curriculum irregolari secondo la Luiss Business School

3
LAUREE FALSE
Inserite nel cv da Marilee Jones che al Mit controllava proprio i titoli dei candidati

I numeri

I LIVELLI DI ISTRUZIONE E I RITORNI OCCUPAZIONALI
PER CLASSI DI ETÀ

IL CONFRONTO INTERNAZIONALE
I LAUREATI



dificabile di titoli e competenze creato con la tecnologia Blockchain. In Italia la prima a investire in questo settore è la Luiss Business School: a partire dal prossimo settembre, istituirà su una piattaforma Blockchain una sorta di "registro" dei corsi conseguiti presso di essa, sia master tradizionali che "executive", cioè quei corsi riservati a chi è già laureato, di solito ha anche già un lavoro, però vuole arricchire il curriculum puntando su nuove e più gratificanti offerte. «L'applicazione della Blockchain alla formazione executive è un punto di svolta per noi e per il settore», commenta Paolo Boccardelli, che della Luiss Business School è il direttore. «Attraverso il digitale cambiamo il modo di lavorare e saremo in grado di determinare profondi cambiamenti nel mercato del lavoro e dell'educazione, introducendo un livello di trasparenza fino a ieri inimmaginabile». Il registro istituirà per ogni "allievo" una vera e propria scheda personale, completandola con tutte le informazioni anagrafiche e professionali. Così le aziende e le istituzioni saranno in grado di conoscere nel dettaglio il percorso, la formazione e soprattutto le competenze delle persone - i punti in cui l'allievo si è particolarmente distinto nei suoi studi e le varie specializzazioni conseguite - e questo sarà

L'opinione

Decine i casi illustri in ogni Paese di curriculum universitari contestati: persino la nuova presidente della commissione Ue, Ursula von der Leyen, è finita in un pasticcio del genere

I CASI ITALIANI

In Italia casi del genere ce ne sono ovviamente a bizzeffe, dal sottosegretario Guido Crosetto che ammise «l'innocente bugia» di essersi inventato una laurea in Economia a Renzo Bossi che si era laureato all'università privata Kristal di Tirana senza aver preso la maturità,

Con la nuova tecnologia Blockchain chi avrà studiato alla Luiss Business School avrà i titoli e anche le competenze acquisite "validati" con assoluta certezza

Annette Schavan era ministra da Educação em 2013, quando a Universidade de Dusseldorf a acusou de ter plagiado sua tese de doutorado.

Giuseppe Conte era primeiro-ministro da Itália em 2018, quando a New York University revelou que nunca havia se matriculado no mestrado em administração que alegava ter obtido.

A Luiss Business School de Roma descobriu que 85% dos currículos contêm informações falsas.

Portanto, decidiu criar um registro digital permanente contendo todas as informações sobre cada aluno, desde a matrícula até a morte e acessível em um ambiente de nuvem, e utilizando o *blockchain* como seu principal instrumento de autenticação.

Esta é uma decisão sensata?

Conceitos básicos

SIMPÓSIO INTERNACIONAL DE ARQUIVOS
Arquivo, documento e informação em cenários híbridos.
5 A 13 DE DEZEMBRO DE 2020

Conforme Jenkinson:

Documento de arquivo é qualquer documento produzido ou recebido (isto é, criado) no decorrer de atividades e conservado para posterior uso ou referência.

- Por ser um documento (ou seja, informação fixada em um suporte), o documento de arquivo possui conteúdo estável e forma fixa.
- Em razão das circunstâncias de sua criação, o documento de arquivo é natural (um subproduto da atividade), inter-relacionado (vinculado a outros), imparcial (não criado para responder a perguntas que pesquisadores possam fazer no futuro) e autêntico (com relação ao criador, se usado como instrumento de uma atividade).
- Preservar um documento de arquivo significa garantir sua estabilidade física e/ou tecnológica (com a finalidade de estender sua vida útil indefinidamente) e proteger seu conteúdo intelectual e seus vínculos com outros documentos.
- A preservação digital é o processo para manter autênticos e acessíveis os materiais digitais durante e entre diferentes gerações de tecnologia ao longo do tempo, independentemente de onde são armazenados.

Características dos documentos de arquivo nato-digitais

SIMPÓSIO INTERNACIONAL DE ARQUIVOS
Arquivo, documento e informação em cenários híbridos.
5 A 13 DE DEZEMBRO DE 2020

- Conteúdo, estrutura e forma desses documentos não estão inextricavelmente ligados.
- Como entidades armazenadas, tais documentos são distintos de sua manifestação na tela de um computador, e seus componentes digitais devem ser considerados, bem como sua forma documental.
- Eles são vulneráveis (podem facilmente ser destruídos, perdidos, corrompidos e adulterados, tornando-se inacessíveis sem a devida proteção), embora persistentes (existirão para sempre, desde que não sejam destruídos propositalmente).
- Quando salvamos um documento, nós o desmembramos em seus componentes digitais. Quando o recuperarmos, criamos uma cópia: não existem originais no ambiente digital.
- Portanto, não é possível preservar os documentos digitais originais: só podemos preservar a capacidade de reproduzi-los ou de recriá-los.

Da imparcialidade e autenticidade à credibilidade do documento de arquivo

SIMPÓSIO INTERNACIONAL DE ARQUIVOS
Arquivo, documento e informação em cenários híbridos.
5 A 13 DE DEZEMBRO DE 2020

Confiabilidade

Credibilidade de um documento como uma **declaração de fato,** *com base*

- na competência de seu autor
- nos controles sobre sua criação

Precisão

Correção e exatidão dos dados de um documento, *com base*

- na competência de seu autor
- nos controles sobre o documento e a transmissão de seu conteúdo

Autenticidade

Credibilidade de um documento que **é o que aparenta ser**, não adulterado e não corrompido, *com base*

- *em sua identidade*
- *em sua integridade*

Identidade

SIMPÓSIO INTERNACIONAL DE ARQUIVOS
Arquivo, documento e informação em cenários híbridos.
5 A 13 DE DEZEMBRO DE 2020

A *identidade* refere-se aos atributos que caracterizam com exclusividade um documento de arquivo, distinguindo-o de outros documentos. Esses atributos incluem:

- os **nomes** das pessoas que participaram de sua criação (isto é, autor, destinatário, redator, produtor, criador);
- a(s) **data(s)** de criação (isto é, produção, recepção, arquivamento) e transmissão;
- o evento ou a **ação** de que participa;
- a expressão de seus **relacionamentos** com outros documentos (por exemplo, o código de classificação); e
- a indicação de eventuais **anexos**.

Integridade

SIMPÓSIO INTERNACIONAL DE ARQUIVOS
Arquivo, documento e informação em cenários híbridos.
5 A 13 DE DEZEMBRO DE 2020

A *integridade* refere-se ao fato de estar completo e inalterado em todos os aspectos essenciais.

Nunca fomos muito exigentes com relação a tal qualidade. E se um documento apresentar furos, queimaduras em um dos lados, ou se a tinta tiver vazado?

A mesma definição de integridade tem sido usada para dados, documentos, cópias, sistemas de arquivo, sem grandes problemas... mas até que ponto isso é válido em ambientes digitais?

Perda de integridade: documento analógico

Perda de integridade: documento digital

- Se os bits originais forem 101
- Transformá-los em 110
- Ou em 011

- Significa manter os mesmos bits

Mas com valores diferentes

Integridade bit a bit

SIMPÓSIO INTERNACIONAL DE ARQUIVOS
Arquivo, documento e informação em cenários híbridos.
5 A 13 DE DEZEMBRO DE 2020

Frequentemente identificado com **Integridade de Dados:**

- *Os dados no documento não são modificados intencionalmente ou acidentalmente*
- *Os **bits originais mantêm-se em estado completo e inalterado** desde o momento da captura, ou seja, eles possuem exatamente a mesma ordem e valor*

Uma pequena modificação em um bit significa um valor muito diferente, tanto no que se vê na tela quanto no que se processa em um programa ou banco de dados.

Integridade da duplicação

SIMPÓSIO INTERNACIONAL DE ARQUIVOS
Arquivo, documento e informação em cenários híbridos.
5 A 13 DE DEZEMBRO DE 2020

O processo de criação de uma cópia não modifica o documento (intencional ou acidentalmente), pois o resultado é uma cópia com os mesmos bits do conjunto original de dados (dados de forma, conteúdo e composição).

A integridade da duplicação é **ligada ao tempo**, e deve-se considerar o uso de carimbos de data/hora para esse fim.

Mas, no ambiente digital, quando dizemos duplicação, precisamos ser explícitos sobre o que queremos dizer, cópia ou imagem?

Duplicação: cópia

SIMPÓSIO INTERNACIONAL DE ARQUIVOS
Arquivo, documento e informação em cenários híbridos.
5 A 13 DE DEZEMBRO DE 2020

Duplicação seletiva (por ex., PDF)

- Só copia o que se vê
- Raramente inclui confirmação de completude
- Fornece imagem incompleta do ambiente

Duplicação: imagem

SIMPÓSIO INTERNACIONAL DE ARQUIVOS
Arquivo, documento e informação em cenários híbridos.
5 A 13 DE DEZEMBRO DE 2020

Duplicação forense:

Reprodução bit a bit do meio de armazenamento e de seu conteúdo, incluindo dados ambientais (por ex., fotos de cada arquivo aberto), espaço de troca (memória virtual, com senhas e chaves de criptografia) e espaço livre (com material excluído).

Integridade do processo de duplicação: princípios

SIMPÓSIO INTERNACIONAL DE ARQUIVOS
Arquivo, documento e informação em cenários híbridos.
5 A 13 DE DEZEMBRO DE 2020

Princípio de não-interferência: o método usado para reproduzir ou recriar um documento digital não altera as entidades digitais.

Princípio de interferência identificável: se o método usado altera as entidades, as mudanças são identificáveis e identificadas (incluindo paradados).

Autenticação

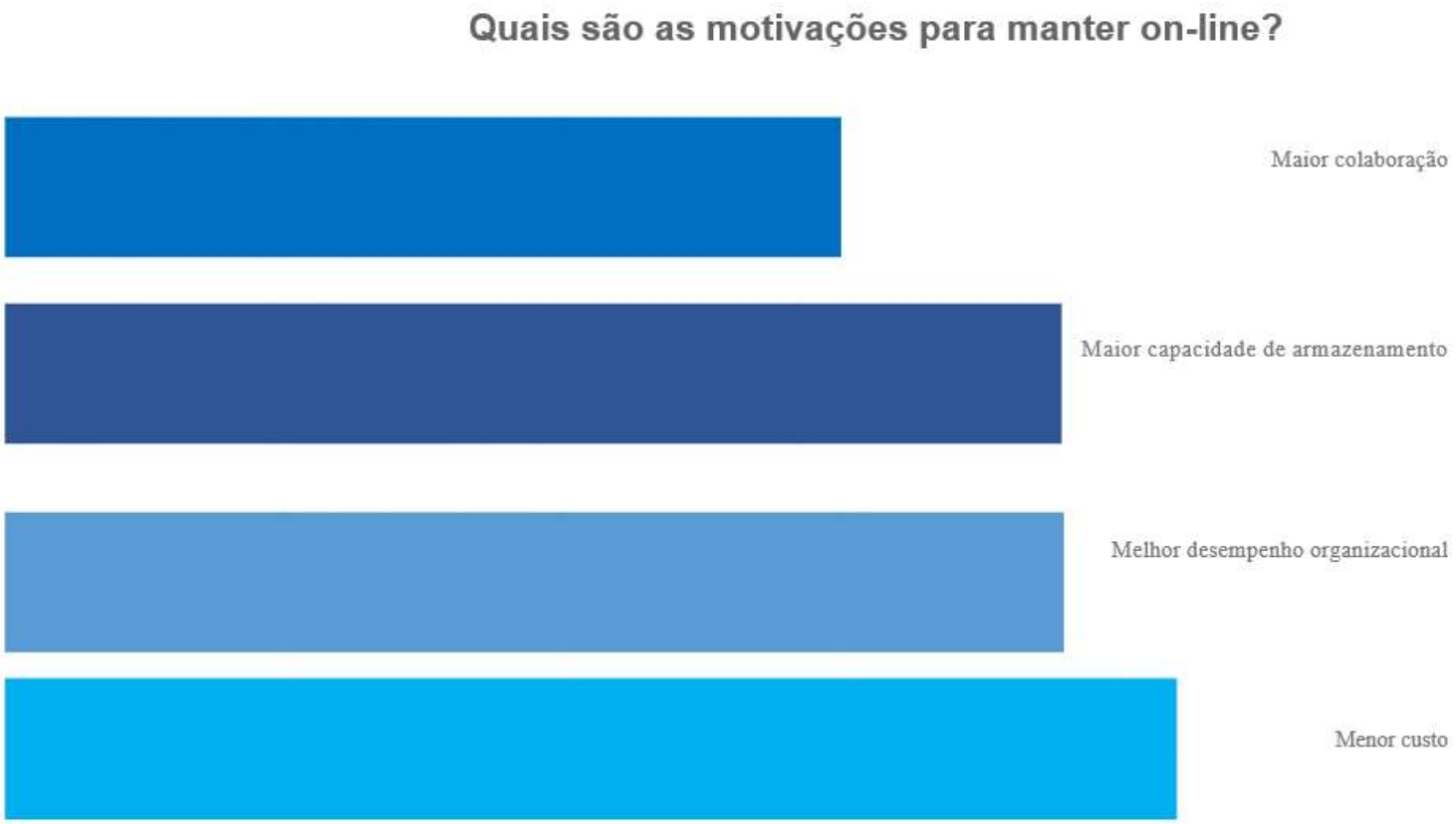
SIMPÓSIO INTERNACIONAL DE ARQUIVOS
Arquivo, documento e informação em cenários híbridos.
5 A 13 DE DEZEMBRO DE 2020

Definição: Declaração de autenticidade baseada em conhecimento direto, prova material, inferência ou dedução.

Base para autenticação de documentos digitais

- A cadeia de custódia legítima permanece sendo a base (base esta cada vez mais significativa!) para inferir autenticidade e autenticar um documento (Jenkinson! cadeia de custódia ininterrupta).
- **Cadeia de custódia digital:** informação sobre o documento arquivístico e suas alterações que é preservada e que demonstra que dados específicos encontravam-se em determinado estado, numa certa data e num certo horário.
- **Declaração** feita por um especialista que se baseia na confiabilidade do sistema que abriga o documento e nos procedimentos e processos que controlam sua preservação e seu uso.

Documentos na nuvem



Problemas

- *Propriedade dos dados*
- *Disponibilidade, acesso e confiabilidade*
- *Retenção e destinação*
- *Armazenamento e manutenção*
- *Segurança*
- *Localização e transferência*
- *Fim do serviço*
- *Preservação*
- *Credibilidade*

SIMPÓSIO INTERNACIONAL DE ARQUIVOS
Arquivo, documento e informação em cenários híbridos.
5 A 13 DE DEZEMBRO DE 2020

Propriedade de dados

- Quando um usuário confia seus documentos a um provedor e usa a plataforma e os aplicativos deste provedor para gerar dados adicionais, o **provedor criará dados** relacionados a ações de processamento, gerenciamento etc.

- Embora o conteúdo criado e/ou armazenado na nuvem pelo usuário seja de sua propriedade, **os metadados criados pelo provedor não o são**, e, como o usuário precisa deles para demonstrar a integridade dos documentos, os acordos contratuais devem determinar se e como o usuário possui o **direito de acesso e uso dos metadados do provedor.**

Disponibilidade, acesso, confiabilidade

SIMPÓSIO INTERNACIONAL DE ARQUIVOS
Arquivo, documento e informação em cenários híbridos.
5 A 13 DE DEZEMBRO DE 2020

- Disponibilidade é um fato, ao passo que acesso é um direito. Mas este não pode ser usufruído sem aquele.

- Em um ambiente de nuvem, a **disponibilidade dos arquivos armazenados** implica também a **disponibilidade da infraestrutura** (i.e., o percentual de tempo que se espera que um sistema fique em operação é de 100%), o que facilita a recuperação e legibilidade dos dados. As dificuldades técnicas podem atrasar um processo baseado na Lei de Acesso à Informação, e o proprietário dos dados, sendo responsável por conceder acesso aos mesmos, pode ser punido.

- Confiabilidade é a característica de se comportar de forma consistente com as expectativas: deve-se considerar não apenas a disponibilidade dos documentos por meio de redundância, mas também a **consistência e a precisão** de acesso.

Retenção e destinação de documentos

SIMPÓSIO INTERNACIONAL DE ARQUIVOS
Arquivo, documento e informação em cenários híbridos.
5 A 13 DE DEZEMBRO DE 2020

- Conformidade é difícil de verificar.

- **a transferência** de um sistema para outro para fins de retenção pode envolver a perda de autenticidade

- **o descarte** pode envolver:

  - *violação de confidencialidade ou privacidade,*
  - *persistência de algumas das cópias e metadados relacionados, e*
  - *persistência dos metadados gerados pelo provedor sobre os dados do usuário.*

Armazenamento e manutenção de documentos

SIMPÓSIO INTERNACIONAL DE ARQUIVOS
Arquivo, documento e informação em cenários híbridos.
5 A 13 DE DEZEMBRO DE 2020

- O armazenamento e a manutenção impactam a qualidade dos documentos e sua capacidade de servir como prova jurídica, especialmente em países onde a autenticidade do documento é uma inferência feita a partir da integridade do sistema em que residem os dados (Conselho de Normas do Governo do Canadá 74:32 2017).

- Os contratos geralmente não especificam como os documentos serão mantidos em meio a tecnologias e formatos de dados em constante evolução, e geralmente definem que os usuários são responsáveis por guardar becape de seus dados. Todos os procedimentos de manutenção, incluindo armazenamento adequado, cuidado, custódia e controle de dados, são chamados pelos fornecedores de "procedimentos de becape".

Segurança dos documentos

SIMPÓSIO INTERNACIONAL DE ARQUIVOS
Arquivo, documento e informação em cenários híbridos.
5 A 13 DE DEZEMBRO DE 2020

- *É a proteção do sistema ou dos documentos contra **acesso, uso, alteração ou destruição não autorizados.** Em um mundo em que a integridade de um sistema é uma inferência da qual se presume a integridade do documento, a partir do qual se pode inferir sua autenticidade e, em seguida, sua confiabilidade, **segurança é a nova autenticidade**.*

- *As pessoas reforçam a segurança com algo que conhecem (por ex., uma senha), que possuem (por ex., tokens), ou que são (por ex., biometria de olhos, impressões digitais, chaves privadas em um ambiente PKI).*

- *O provedor de nuvem a mantém por meio de criptografia e deve **produzir trilhas de auditoria e registros de acesso**, e capturar, manter e disponibilizar **metadados** associados ao acesso, à recuperação, ao uso e à gestão dos dados, além daqueles ligados aos próprios dados.*

- ***O problema de segurança está diretamente relacionado à localização dos dados e ao fluxo entre os dados.***

Localização e transferência de documentos

SIMPÓSIO INTERNACIONAL DE ARQUIVOS
Arquivo, documento e informação em cenários híbridos.
5 A 13 DE DEZEMBRO DE 2020

- *A nuvem é a plataforma de preferência para aplicativos móveis e para os dados gerados com seu uso, bem como para aqueles criados em dispositivos inteligentes. Os documentos podem estar em centros de dados em qualquer lugar do mundo.*

- *A localização dos documentos é um dos critérios usados para determinar a lei aplicável em caso de litígio.*

- *Estratégias nacionais costumavam exigir que os documentos residissem dentro das fronteiras do país onde foram criados (muito caro para centros de dados, se localizados na Europa ou América do Norte).*

- *A estratégia internacional já não exige mais isso, o que aumenta a importância dos acordos multilaterais entre países para colaboração em segurança (novo porto seguro).*

Fim de serviço: rescisão contratual

SIMPÓSIO INTERNACIONAL DE ARQUIVOS
Arquivo, documento e informação em cenários híbridos.
5 A 13 DE DEZEMBRO DE 2020

- Se o provedor deixar de existir ou encerrar um ou mais de seus serviços (por violação, inatividade ou conveniência), os documentos serão apagados ou ficarão inacessíveis.

- Os serviços gratuitos não têm duração determinada e podem encerrar contas unilateralmente, obrigando os usuários a excluir *softwares* e aplicativos, e prevenindo que acessem os dados que permanecerem com o provedor.

- Quando os dados são devolvidos ao usuário, não é certo que eles estarão em um formato utilizável e interoperável.

- Caso o contrato seja rescindido pelo usuário, a restituição dos dados pode ser cara, e os dados podem não estar em formatos acessíveis. Além disso, o usuário pode não ter o direito de acesso aos metadados gerados pelo sistema para sua manutenção de documentos ou fins legais, e pode não haver nenhuma garantia de que o provedor irá destruir todas as cópias dos dados mantidos em seus centros de dados.

Preservação de documentos

SIMPÓSIO INTERNACIONAL DE ARQUIVOS
Arquivo, documento e informação em cenários híbridos.
5 A 13 DE DEZEMBRO DE 2020

- Preservar documentos na nuvem é um **processo de caixa preta.**
- Os provedores **podem não saber onde estão os documentos** e podem **subcontratar** alguns serviços de outros provedores, mantendo provedores em diferentes países.
- Não se pode esperar que os mesmos *hardware* e *software* permanecerão em operação pelo tempo em que os documentos devem ser preservados, ou que as tecnologias que os substituirão serão **compatíveis** com as anteriores.
- As normas fornecem informações sobre os formatos de preservação, mas **não há como controlar a conformidade.**
- Não há como controlar a **credibilidade.**

Autenticação

SIMPÓSIO INTERNACIONAL DE ARQUIVOS
Arquivo, documento e informação em cenários híbridos.
5 A 13 DE DEZEMBRO DE 2020

Definição: Declaração de autenticidade baseada em conhecimento direto, prova material, inferência ou dedução.

Base para autenticação de documentos digitais

- **A cadeia de custódia legítima** permanece sendo a base (base esta cada vez mais significativa!) para inferir autenticidade e autenticar um documento (Jenkinson! cadeia de custódia ininterrupta).
- **Cadeia de custódia digital:** informação sobre o documento arquivístico e suas alterações que é preservada e que demonstra que dados específicos encontravam-se em determinado estado, numa certa data e num certo horário.
- Uma **declaração** feita por um especialista, que se baseia na confiabilidade do sistema que abriga o documento e nos procedimentos e processos que controlam sua preservação e seu uso.

Autenticação dependente de tecnologia

SIMPÓSIO INTERNACIONAL DE ARQUIVOS
Arquivo, documento e informação em cenários híbridos.
5 A 13 DE DEZEMBRO DE 2020

Assinatura digital:

- protege a **integridade de bits;**
- verifica a origem de um documento (parte de sua **identidade**), torna o documento indiscutível e incontestável (**não-repúdio**);
- recebeu valor jurídico por meio de atos legislativos (por ex., Diretriz Europeia sobre assinaturas eletrônicas) ou órgãos reguladores (Comissão de Valores Mobiliários sobre funções ***hash***);
- é habilitada por meio de infraestruturas de chave pública (PKI) complexas e caras;
- garante a autenticidade das informações através do espaço, mas não do tempo!
- é sujeita à obsolescência e agrava o problema de preservação, uma vez que não pode ser migrada com o documento ao qual está anexada, e os certificados têm data de validade;
- A teoria diz que tem a função de um **selo**, e não de uma assinatura, de modo que pode ser removida e substituída por metadados.

Autenticação dependente de tecnologia

SIMPÓSIO INTERNACIONAL DE ARQUIVOS
Arquivo, documento e informação em cenários híbridos.
5 A 13 DE DEZEMBRO DE 2020

Tecnologia de ***blockchain:***

- *a te*cnologia por trás do *bitcoin;*
- um livro-razão, ou seja, um armazenamento de informações que mantém um rastreio final e definitivo (imutável) de transações (*hash*).

Depende de uma rede distribuída (todos os nódulos/servidores são iguais) e consenso descentralizado (nenhum centro de dados; nenhum ponto único de controle ou ataque).

Os conjuntos de transações confirmadas e validadas são mantidos em blocos, que são ligados (encadeados) numa cadeia que é resistente a adulterações e só permite anexação.

Começa com um bloco original, e cada bloco contém, além do *hash* de um número predeterminado de documentos, um *hash* do bloco anterior na cadeia.

Como o *blockchain* é usado?

SIMPÓSIO INTERNACIONAL DE ARQUIVOS
Arquivo, documento e informação em cenários híbridos.
5 A 13 DE DEZEMBRO DE 2020

O *blockchain* pode ser usado para confirmar

- a integridade de um documento mantido em outro lugar;
- que um documento existiu ou foi criado em um determinado ponto no tempo (ou seja, não depois de ser marcado com o carimbo de data/hora e registrado no *blockchain*);
- a sequência de *uploads* de documentos para o *blockchain.*

É um **sistema de gestão de documentos**? Não. Ele contém o *hash* dos documentos, mas não os documentos em si (contratos inteligentes - acordos entre as partes gravados diretamente em linhas de código - não são documentos. Os documentos ainda precisam ser armazenados e gerenciados fora da cadeia. Isso é bom, porque, se eles estivessem no *blockchain*, seriam imutáveis.

Imutabilidade/integridade

SIMPÓSIO INTERNACIONAL DE ARQUIVOS
Arquivo, documento e informação em cenários híbridos.
5 A 13 DE DEZEMBRO DE 2020

- *É o atrativo do blockchain: é o que garante a integridade, pois nada pode ser alterado em um documento ou removido de um bloco.*

- *É o principal problema do blockchain:*

– *com **documentos correntes**, qualquer **atualização ou correção** de dados errados; qualquer forma de **proteção de privacidade;** qualquer exercício do **direito de ser esquecido;** qualquer **descarte** de documentos não mais necessários; qualquer **atualização do sistema de produção de documentos**; em resumo, qualquer mudança no(s) documento(s) invalidaria o blockchain;*

– *com **documentos identificados para preservação continuada**, qualquer **transferência** para um sistema de preservação; qualquer **migração;** qualquer **acréscimo** ao conjunto de documentos invalidaria o blockchain.*

Identidade

- *O hash no blockchain não permite links para*
  - o *hash* de documentos relacionados, portanto não há vínculo arquivístico;
  - o *hash* de metadados, portanto não há contexto.
- *Se os metadados fossem incorporados ao documento na criação, o hash desse documento não permitiria acréscimos ou alterações.*

Problemas legais com documentos autenticados em *blockchain*

SIMPÓSIO INTERNACIONAL DE ARQUIVOS
Arquivo, documento e informação em cenários híbridos.
5 A 13 DE DEZEMBRO DE 2020

- *Comprovação de **confiabilidade, acurácia** e **autenticidade na origem** (imparcialidade e autenticidade do documento).*
- *Preservação de **provas contextuais** (a naturalidade e inter-relação dos documentos resultantes de um processo).*
- *Como lidar com a natureza **descentralizada** (e, consequentemente, transjurisdicional) do blockchain (quem é o criador? o autor? o proprietário? qual lei se aplica?).*
- *Lidar com o código em uma situação em que os componentes necessários da transação são controlados por diferentes atores em diferentes jurisdições; e com **contratos inteligentes**, sem qualquer equivalente de assinatura ou data de conclusão do contrato.*

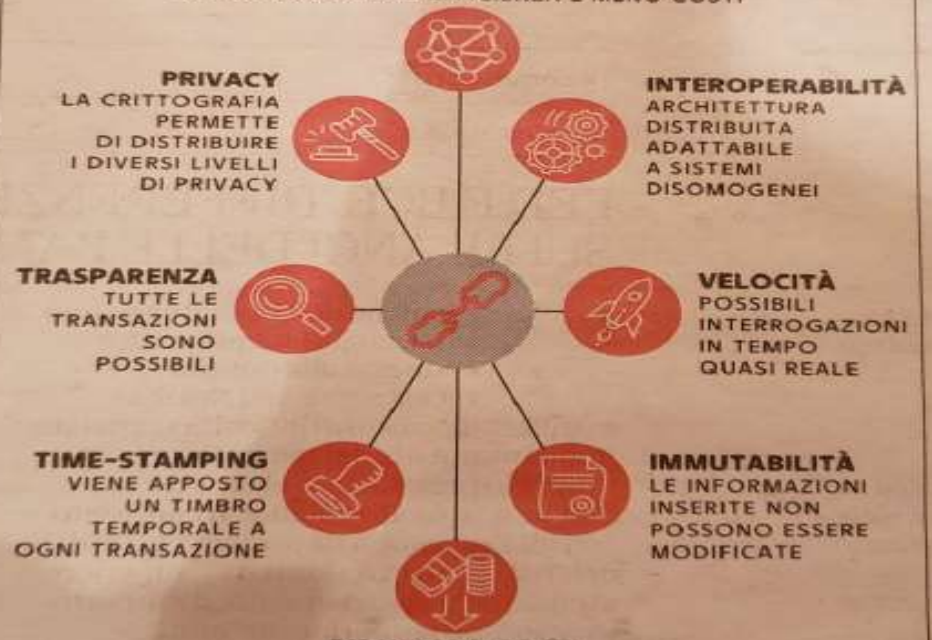
valido dall'impiegato al top executive. «Gli sviluppi della Blockchain sono ancora per molti versi inesplorati», aggiunge Boccardelli. Non a caso uno dei corsi abilitanti della Luiss Business School, i cui risultati saranno ovviamente riportati nel "registro" hi-tech, sarà dedicato proprio alle tecnologie Blockchain, a fianco di tante altre specializzazioni, dalle filiere agroalimentari al Fintech.

LA SOCIETÀ DI HI-TECH

Il partner tecnologico è EY, che a sua volta punta fortemente su questa tecnologia al punto di avervi dedicato venti centri d'eccellenza in tutto il mondo. Giuseppe Perrone, responsabile dell'"hub" dedicato alla Blockchain di Roma, l'unico in Italia, che serve l'intera area del Mediterraneo, spiega: «Abbiamo scelto fra le poche piattaforme d'appoggio esistenti nel mondo la Ethereum, sicuramente ai vertici fra le reti di Blockchain pubbliche, cioè consultabili da chiunque via Internet. Ad essa come EY facciamo spesso riferimento per le aziende nostre partner». Il "pacchetto" predisposto per la Luiss prevede che non venga certificata solo l'attività svolta presso l'università. «Ricostruiamo l'intera vita professionale dell'interessato, inserendo nel registro non solo i titoli ma tutte le competenze acquisite, ovviamente con il suo consenso, e inseriamo il tutto nel curriculum che acquisisce così una ben superiore affidabilità», spiega Enzo Peruffo, responsabile della Executive education alla Luiss Business School. Ma chi certifica i certificatori della Blockchain? «La procedura di Ethereum – riprende Perrone - è la seguente. Essendo un network, i vari "nodi" che la compongono sono fra di loro indipendenti. A ogni "nodo" corrisponde un server, abbastanza potente da essersi guadagnato il titolo di "miner". Al momento di comporre il "token", cioè l'identità a cui poi corrisponderà un codice, di uno studente Luiss, uno di questi "nodi" acquisisce una sorta di leadership. Ad esso però, con una serie di passaggi che avvengono in pochissimi secondi, se ne aggiungono altri sei, ognuno dei quali fa le sue verifiche e poi concorre alla "bollinatura" del candidato. Un sistema di controlli e validazione ampiamente sperimentato che secondo noi garantisce la totale affidabilità e trasparenza di questa certificazione».

I numeri

LE VIRTÙ DELLA BLOCKCHAIN
PRINCIPALI VANTAGGI



Um uso ilimitado?

SIMPÓSIO INTERNACIONAL DE ARQUIVOS
Arquivo, documento e informação em cenários híbridos.
5 A 13 DE DEZEMBRO DE 2020

A equipe do Archangel Project (TNA, Universidade de Surrey e o Open Data Institute, de Tim Berners-Lee) afirma:

"*Blockchain* é um escudo que os arquivos podem usar para defender os documentos e sua autenticidade. Ao permitir que os pesquisadores comparem o conteúdo das provas (incluindo o *checksum* do documento) com o registrado no *blockchain*, eles podem ver provas de que nenhuma alteração (deliberada ou acidental) foi feita no documento desde que ele foi preservado no arquivo. Além disso, a natureza descentralizada dos *blockchains* elimina a necessidade dos cidadãos confiarem nas instituições individualmente, pois cada um é guardião de outros guardiões."

Problemas de descentralização

SIMPÓSIO INTERNACIONAL DE ARQUIVOS
Arquivo, documento e informação em cenários híbridos.
5 A 13 DE DEZEMBRO DE 2020

- O processamento da informação acontece numa ordem tecnológica complexa na qual diferentes componentes técnicos podem estar sob a custódia de e operados por atores muito diferentes.

- Alguns componentes podem estar sob o controle de uma única organização, outros sob o controle de parceiros comerciais que são membros de um consórcio de *blockchain*, e ainda outros controlados por terceiros desconhecidos.

- Os documentos de uma organização podem estar sob a custódia de milhares de atores independentes sobre os quais os criadores dos documentos exercem pouco ou nenhum controle.

Descentralização (cont.)

- O mecanismo de consenso e outros protocolos ou padrões que determinam como o *blockchain* opera podem não estar incluídos no campo de tomada de decisão do produtor (ou do profissional de arquivo designado pelo produtor).

- Em vez disso, podem ser decididos por desenvolvedores remotos (e até mesmo desconhecidos) terceirizados. Em muitos casos, esses protocolos e padrões ainda são instáveis e, portanto, a confiabilidade do *upload* de documentos organizacionais para o *blockchain* pode ser muito difícil de estabelecer com alguma certeza.

E quanto à descentralização parcial?

Modelo de Preservação InterPARES TRUSTER

- *Sistema baseado em blockchain chamado "TrustChain"*

- *Aplica os conceitos de:*
  - algoritmos *hash*
  - *blockchain*
  - consenso distribuído

- *Premissas:*
  - *blockchain* de nuvem privada
  - apenas nódulos aprovados podem gravar
  - todos podem ler

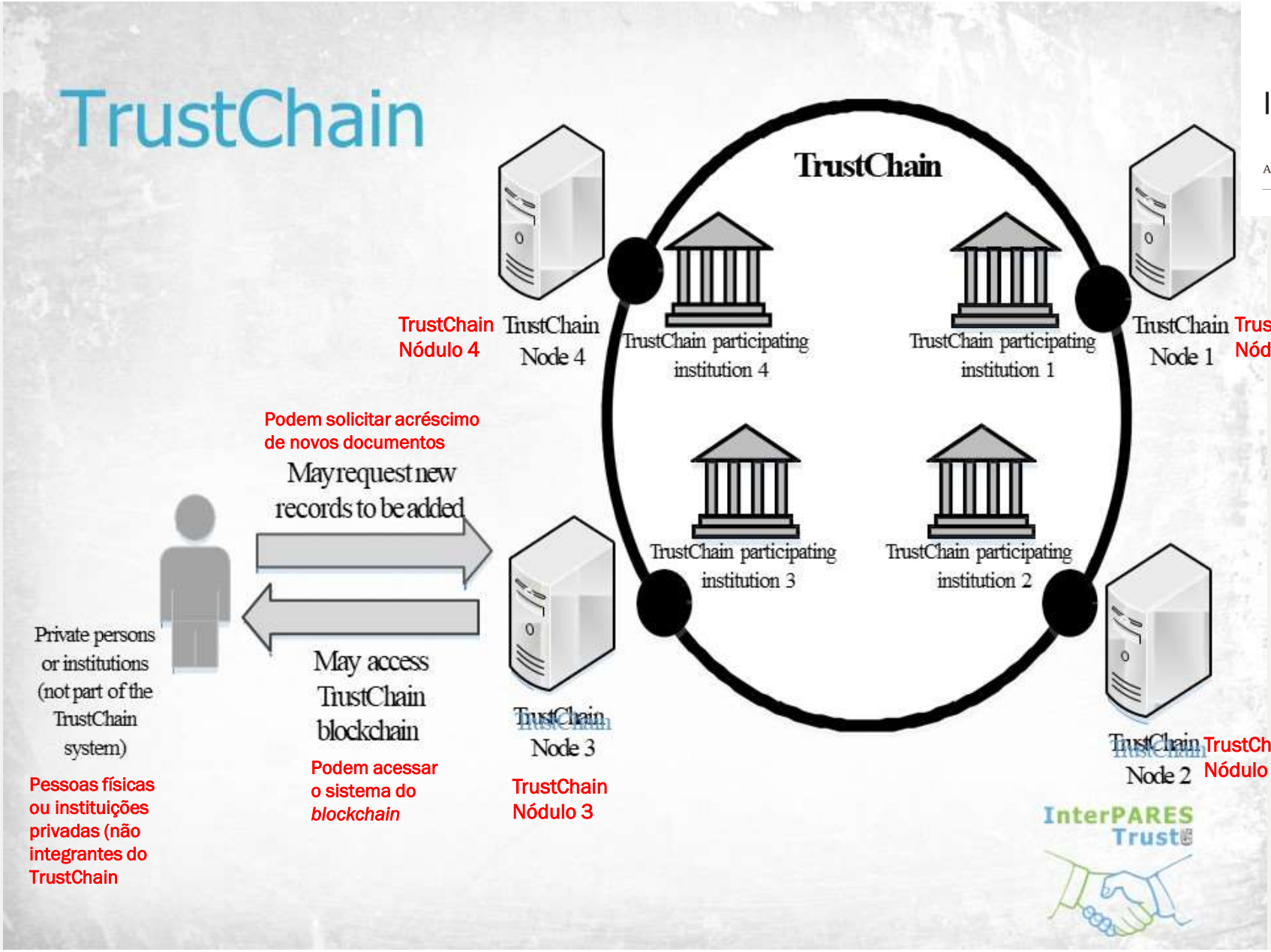
TrustChain

SIMPÓSIO INTERNACIONAL DE ARQUIVOS
Arquivo, documento e informação em cenários híbridos.
5 A 13 DE DEZEMBRO DE 2020

O sistema proposto *TrustChain*

- *depende do envolvimento de um* ***grupo de instituições confiáveis;***
- ***o sistema de gestão de documentos no órgão produtor*** *e* ***o sistema de preservação nos arquivos*** *funcionariam* ***em harmonia*** *ao longo do ciclo de vida dos documentos;*
- *forneceria confirmação de* ***integridade****, tempo de* ***criação/existência, sequência de documentos, não-repúdio, validade de assinaturas eletrônicas*** *cujo certificado estiver dentro da validade.*

TrustChain



TrustChain Nódulo 4

Podem solicitar acréscimo de novos documentos

TrustChain Nódulo 1

Pessoas físicas ou instituições privadas (não integrantes do TrustChain

Podem acessar o sistema do *blockchain*

TrustChain Nódulo 3

TrustChain Nódulo 2

Documentos disruptivos

SIMPÓSIO INTERNACIONAL DE ARQUIVOS
Arquivo, documento e informação em cenários híbridos.
5 A 13 DE DEZEMBRO DE 2020

- No entanto, mesmo o *TrustChain* seria uma situação temporária e cara, pois uma nova cadeia teria que ser gerada a cada etapa do ciclo de vida do documento.

- É por isso que a Dra. Victoria Lemieux da UBC reuniu uma equipe multidisciplinar internacional para redesenhar o *blockchain* como o conhecemos, de forma que os problemas identificados possam ser resolvidos (ver Blockchain@UBC).

- E a University of British Columbia está lançando uma série de treinamentos em tecnologia *blockchain* para estudantes de pós-graduação, o primeiro programa no Canadá. A série se concentrará em quatro áreas: saúde e bem-estar, energia limpa, tecnologia regulatória e questões para comunidades indígenas, lançada oficialmente em janeiro de 2020.

Inteligência artificial

SIMPÓSIO INTERNACIONAL DE ARQUIVOS
Arquivo, documento e informação em cenários híbridos.
5 A 13 DE DEZEMBRO DE 2020

Que tal usar Sistemas de Inteligência Artificial?

SIA são sistemas de computação que empregam algoritmos capazes de realizar tarefas complexas que antes eram consideradas domínio exclusivo da inteligência natural:

processamento de grandes quantidades de informação,

cálculos e **previsões**,

aprendizagem e **adaptação** de respostas a situações em constante mudança,

reconhecimento e **classificação** de objetos.

Por que devemos depender de uma tecnologia quando podemos desenvolver sistemas que executam com competência e eficiência todas as funções arquivísticas, ao mesmo tempo mantendo a credibilidade dos documentos?

Problemas da IA

SIMPÓSIO INTERNACIONAL DE ARQUIVOS
Arquivo, documento e informação em cenários híbridos.
5 A 13 DE DEZEMBRO DE 2020

Oferece:

- Provas inconclusivas (com base em probabilidades);
- Provas inescrutáveis (sem interpretabilidade e transparência);
- Provas equivocadas (tão boas quanto os dados fornecidos);
- Desfechos injustos (impacto desproporcional em um grupo de pessoas);
- Efeitos transformadores (desafios para a autonomia e a privacidade);
- Não rastreabilidade (difícil atribuir responsabilidade).

Mittelstadt e colegas (2016).

E mais:

> *As decisões tomadas pela IA são baseadas em decisões anteriores e*
>
> *quando se trata de assuntos humanos, amanhã raramente se parece com hoje, e dados e números não podem dizer o que tem valor moral, nem o que é socialmente desejável.*

A Declaração de Montreal sobre o Desenvolvimento Responsável da IA

SIMPÓSIO INTERNACIONAL DE ARQUIVOS
Arquivo, documento e informação em cenários híbridos.
5 A 13 DE DEZEMBRO DE 2020

- Oferece um quadro ético que permite a promoção dos direitos humanos reconhecidos internacionalmente nos campos que sofrem impactos com a implantação da inteligência artificial.

- Tomados como um todo, os princípios articulados estabelecem os fundamentos da confiança social nos sistemas de inteligência artificial.

Princípios

SIMPÓSIO INTERNACIONAL DE ARQUIVOS
Arquivo, documento e informação em cenários híbridos.
5 A 13 DE DEZEMBRO DE 2020

Princípio do **bem-estar**

Princípio do **respeito à autonomia**

Princípio da **proteção à privacidade**

Princípio da **solidariedade**

Princípio da **participação democrática**

Princípio da **equidade**

Princípio da **diversidade e da inclusão**

Princípio do **cuidado**

Princípio da **responsabilidade**

Princípio do **desenvolvimento sustentável**

Conclusão: o que aprendemos?

SIMPÓSIO INTERNACIONAL DE ARQUIVOS
Arquivo, documento e informação em cenários híbridos.
5 A 13 DE DEZEMBRO DE 2020

- Ainda precisamos descobrir como desenvolver algoritmos que respeitem consistentemente esses princípios, mas nosso conhecimento profissional pode ajudar-nos a ver os problemas à medida que surjam e a resolvê-los conversando com cientistas da computação.

- Os arquivos e a profissão de arquivista devem continuar a formar a **infraestrutura por meio da qual crenças e valores são defendidos e compreendidos.** Só eles podem garantir que os documentos da sociedade permaneçam naturais, inter-relacionados, imparciais e autênticos - ou seja, dotado de credibilidade, junto com as instituições arquivísticas a que pertencem.

- A única escolha é **apegar-se aos princípios do nosso campo, ao mesmo tempo apoiando o desenvolvimento científico!** Isso pode ser difícil de conseguir, mas “seria imprudente não tentar” (Floridi).

SIMPÓSIO INTERNACIONAL DE ARQUIVOS

Arquivo, documento e informação em cenários híbridos.

5 A 13 DE DEZEMBRO DE 2020

OBRIGADA!

luciana.duranti@ubc.ca