
Cyberlaw by CIJIC, ***Direito: a pensar tecnologicamente.***

# CYBERLAW by CIJIC

**EDIÇÃO N.º IX – MARÇO DE 2020**

**REVISTA CIENTÍFICA SOBRE CYBERLAW DO CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO – CIJIC – DA FACULDADE DE DIREITO DA UNIVERSIDADE DE LISBOA**

**EDITOR:** NUNO TEIXEIRA CASTRO

**SUPORTE EDITORIAL:** EUGÉNIO ALVES DA SILVA e AFONSO FREITAS DANTAS

**PRESIDENTE DO CIJIC:** EDUARDO VERA-CRUZ PINTO



**CIJIC:** CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO

**ISSN 2183-729**

## NOTAS DO EDITOR:

Globalização. Tecnologia e Inteligência artificial. Mobilidade organizacional e individual. Manipulação. A pandemia de Coronavírus. Hoje. O futuro.

Vivemos tempos "*estranhos*". Acutilantes. Irresolutos. Contingentes. Exigentes. O "tema" que nos capta, quase em exclusivo, a atenção, desde o início do ano de 2020, é a pandemia de coronavírus. Aquela dinâmica, rotineira, até agora tida como "garantida" atravessa momentos de grande indeterminação. Hora a hora somos como que bombardeados com números esmagadores: de taxas mundiais galopantes de infectados, doentes em cuidados intensivos, de mortos. No passar deste tempo, diariamente, deambulámos entre um imoderado e célere na disseminação da infecção *versus* um vagaroso e fleumático passo na demonstração de resultados animadores no seu combate. O racional económico de «custo-benefício» geralmente revelaria a perigosidade associada à extrema cautela. Porém na questão, truncada, do coronavírus é diferente[1]. "*Achatar as curvas*", "*Proteger os mais idosos e os mais vulneráveis*", "*Suster a vaga de procura do SNS por forma a dar-lhe tempo para acudir às solicitações*", mesmo que o custo seja o parar da Economia. Global. Entretanto o tempo continua o seu passo. Assim como a epidemia há-de passar.

1 Cass Sunstein @ https://www.bloomberg.com/opinion/articles/2020-03-26/coronavirus-lockdowns-look-smart-under-cost-benefit-scrutiny

E, quando aí chegados, a questão resolutiva a colocar não deverá andar muito longe de um: "*Que mundo esperar do pós-covid19*"?

O avanço da tecnologia, combinando melhores recursos de *hardware* com inteligência artificial, aos quais o Homem socorre, permitiram sequenciar o genoma do COVID-19 em menos de um mês. A inteligência artificial, por exemplo, num contexto, global, de recursos exíguos tem sido testada para suprir lacunas críticas nos recursos de saúde, ajudando à racionalidade da decisão política, alavancando centros de inovação em inteligência artificial, robótica e automação em saúde. Na Ásia[2]. Por agora.

O mesmo avanço tecnológico, por sua vez, no actual cenário de "*guerra*" ao vírus, colocou a ponderação das liberdades fundamentais num estádio de confronto titânico. Recuperando o "*achatar a curva*", um pouco por todo o mundo, os governos, democráticos, colocaram os respectivos países em *lockdown*. Sem cautelas. Entre confinamentos e quarentenas obrigatórias, um recurso parece permitir - em face da falta de meios humanos para controlo efectivo de milhões de cidadãos - fiscalizar o cumprimento das directrizes estatais. A tentação executiva por esse controlo, universal, dos cidadãos preclude a fruição de múltiplas liberdades constitucionalmente consagradas. O racional da discussão que vinha sendo tido até agora[3], deslocou-se, por via do perigo abstracto que a pandemia comporta, da questão securitária *versus* liberdades fundamentais para "*saúde pública*" *versus* liberdades fundamentais.

Um pouco por todo o ocidente democrático, a tónica recursiva tem passado pelo uso da "*vigilância digital* estadual[4]". Tal como um pouco por todo o mundo, direitos humanos fundamentais[5] são colocados em teste face à imposição destas regras "excepcionais". O Estado de emergência tende a permitir, justificando múltiplas

---

2 Eficiência, especialidade, racionalidade, sistemas capacitativos e colaborativos público-privados. O trabalho dos dados ao serviço dos povos. https://www.technologyreview.com/s/614555/ai-in-health-care-capacity-capability-and-a-future-of-active-health-in-asia/

3 « Tribunal Constitucional chumba acesso das secretas a registos de comunicações», @ https://rr.sapo.pt/2019/09/19/politica/tribunal-constitucional-chumba-acesso-das-secretas-a-registos-de-comunicacoes/noticia/165164/

4 Por exemplo: https://www.wsj.com/articles/europe-tracks-residents-phones-for-coronavirus-research-11585301401

5 Por exemplo, no contexto da América do Sul, «Sociedade civil pede que tecnologias usadas devido à pandemia respeitem os Direitos Humanos», @ https://idec.org.br/noticia/sociedade-civil-pede-governos-da-america-latina-e-caribe-que-tecnologias-digitais-aplicadas

intrusões como *adequadas*[6], *necessárias e proporcionais*[7]. A questão, sendo excepcional e de carácter limitada no tempo, deveria ser pacificamente tolerada pelos cidadãos. Afinal, sob o manto de um fundamento como o "*interesse público*" [8] e salvaguarda da "*saúde pública*" até a limitação do escopo de protecção, desde logo, da privacidade de dados pessoais sensíveis claudica[9].

---

6 No parecer 32/2020, a CNPD, delimitando geograficamente a aplicação de videovigilância por drones ao concelho de Ovar, dada a excepcionalidade da cerca sanitária entretanto imposta, reitera que "(…)as restrições aos direitos fundamentais devem limitar-se ao estritamente necessário às finalidades visadas com este sistema de videovigilância ", recomendando, adicionalmente, "que se garanta que a captação de imagens assim realizada salvaguarde a privacidade daqueles que se encontrem nas respectivas habitações", e, "que se garanta o direito de acesso às imagens gravadas , nos termos legalmente previstos", bem como que se adoptem "medidas adequadas a garantir a integridade das imagens gravadas no processo de transferência dos registos(…) para o "contentor de informação encriptado"" . @ https://www.cnpd.pt/home/decisoes/Par/PAR_2020_32.pdf

7 Por exemplo, em Espanha, a AEPD: «(…)*Los fundamentos que legitiman/hacen posible dichos tratamientos son la necesidad de atender las misiones realizadas en interés público, así como la de garantizar los intereses vitales de los propios afectados o de terceras personas.* ***Las finalidades para las que pueden tratarse los datos son, únicamente, las relacionadas con el control de la epidemia****, entre ellas, las de ofrecer información sobre el uso de las aplicaciones de autoevaluación realizadas por las administraciones públicas o la obtención de estadísticas con datos de geolocalización agregados para ofrecer mapas que informen sobre áreas de mayor o menor riesgo.* ***Los datos que pueden obtenerse y utilizarse han de ser los que las autoridades públicas competentes consideren proporcionados/necesarios para cumplir con dichas finalidades.*** *Estos datos sólo podrán ser facilitados por quienes sean mayores de 16 años. En el caso de tratar datos de menores de 16 años, se requeriría de la autorización de sus padres o representantes legales.* ***Únicamente podrán tratar dichos datos las autoridades públicas competentes para actuar conforme a la declaración del estado de alarma****, es decir, el Ministerio de Sanidad y las Consejerías de Sanidad de las Comunidades Autónomas, que podrán cederse datos entre ellas, y a los profesionales sanitarios que traten a los pacientes o que intervengan en el control de la epidemia.****Las entidades privadas que colaboren con dichas autoridades sólo podrán utilizar los datos conforme a las instrucciones de estas y, en ningún caso, para fines distintos de los autorizados.»*** @ https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/aepd-apps-webs-autoevaluacion-coronavirus-privacidad

8 A limitação ao tratamento de dados sensíveis, por exemplo, de saúde sucumbe ante "*razões de interesse público nos domínios da saúde pública*", desde que «(…)***Tais atividades de tratamento de dados sobre a saúde autorizadas por motivos de interesse público não deverão ter por resultado que os dados sejam tratados para outros fins por terceiros, como os empregadores ou as companhias de seguros e entidades bancárias»*** (Considerando 54 in fine) .

Considerando *(54) « O tratamento de categorias especiais de dados pessoais pode ser necessário por razões de interesse público nos domínios da saúde pública, sem o consentimento do titular dos dados. Esse tratamento deverá ser objeto de medidas adequadas e específicas, a fim de defender os direitos e liberdades das pessoas singulares. Neste contexto, a noção de «saúde pública» deverá ser interpretada segundo a definição constante do Regulamento (CE) n.o 1338/2008 do Parlamento Europeu e do Conselho (11), ou seja, todos os elementos relacionados com a saúde, a saber, o estado de saúde, incluindo a morbilidade e a incapacidade, as determinantes desse estado de saúde, as necessidades de cuidados de saúde, os recursos atribuídos aos cuidados de saúde, a prestação de cuidados de saúde e o acesso universal aos mesmos, assim como as despesas e o financiamento dos cuidados de saúde, e as causas de mortalidade(…)****».***

9 Confirmando o Considerando (54), ainda, da leitura conjunta **das alíneas g) e i) do Art.o 9, n.º2, RGPD**: «**G)** *Se o tratamento for necessário por motivos de interesse público importante, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados*;», e**, i)** « *Se o tratamento for* ***necessário por motivos de interesse público no domínio da saúde pública, tais como a proteção contra ameaças transfronteiriças graves para a saúde*** *ou para assegurar um elevado nível de qualidade e de*

Mas há um "*senão*". O receio de que a excepcionalidade vire regra é real[10]. Com efeito, é inegável que, neste momento, os receios de Yuval Harari [11], criador de *Homo Deus*, sejam partilhados por muitos de nós. Tal como as considerações de Joel P. Trachtman, quanto aos benefícios de um mundo global[12]: benéfico se mais cooperativo, com capacidades regulatórias internacionais reforçadas ao nível da saúde, cibersegurança, proteção ambiental e crises financeiras.

Ambos convergem na necessidade de compromisso, de partilha, cooperação e solidariedade global. O que se conclui espontaneamente dos apontamentos citados, através de um silogismo categórico: ameaça sobre todos os países, ameaça global, logo, resposta de todos os países, global. Não obstante, será que hoje temos líderes políticos mundiais à altura dos desafios[13] pungentes que se nos colocam nestes termos?

E no futuro?

---

*segurança dos cuidados de saúde e dos medicamentos ou dispositivos médicos, com base no direito da União ou dos Estados-Membros que preveja medidas adequadas e específicas que salvaguardem os direitos e liberdades do titular dos dados, em particular o sigilo profissional*;». @ https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679

10 Yuval Harari:«(…) *Many short-term emergency measures will become a fixture of life. That is the nature of emergencies. They fast-forward historical processes. Decisions that in normal times could take years of deliberation are passed in a matter of hours. Immature and even dangerous technologies are pressed into service, because the risks of doing nothing are bigger.", @* https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75

11 Harari: «(…) *In this moment of crisis, the crucial struggle takes place within humanity itself. If this epidemic results in greater disunity and mistrust among humans, it will be the virus's greatest victory. When humans squabble – viruses double. In contrast, if the epidemic results in closer global cooperation, it will be a victory not only against the coronavirus, but against all future pathogens*.», @ https://time.com/5803225/yuval-noah-harari-coronavirus-humanity-leadership/

12 Joel P. Trachtman, «(…) *Not all global problems result from globalization. For those that do, globalization itself can ameliorate them to some extent. Furthermore, we can establish international laws and institutions to minimize those problems that do arise from globalization: globalized governance to respond to globalization-induced problems. This is smart globalization, and once we do it this way, it is likely that globalization should be retained because, on net, it will make us better off*.", @ https://www.bostonglobe.com/2020/03/30/opinion/not-all-global-problems-result-globalization/

13 Ainda Harari: «(…)*Today humanity faces an acute crisis not only due to the coronavirus, but also due to the lack of trust between humans. To defeat an epidemic, people need to trust scientific experts, citizens need to trust public authorities, and countries need to trust each other. Over the last few years, irresponsible politicians have deliberately undermined trust in science, in public authorities and in international cooperation. As a result, we are now facing this crisis bereft of global leaders that can inspire, organize and finance a coordinated global response*.», *idem*.

Gerd Leonhard, num exercício curioso reproduzido no Diário de Notícias, destaca dois aspectos cruciais. Circunscrevendo-nos à tecnologia, esta *"tornou-se a nova religião"*. "*Estamos a entrar num novo Renascimento*". *O próximo passo será regulamentá-la de forma mais apertada com o objetivo de que humanos e o próprio planeta beneficiem do progresso tecnológico.* Não obstante, esta relação acabará seduzir-se ante uma *vigilância estatal por meios tecnológicos* (que) *irá tornar-se o novo normal após as medidas extraordinárias que foram tomadas para controlar esta pandemia*[14].

E como já vai longo, para concluir, convocamos, novamente, a questão fundamental: "*Que mundo esperar do pós-covid19*"?

A provocação desconcertante e acutilante que se impõe, inclusive politicamente, não poderia ser outra: «*Of course, even if we disappear, it will not be the end of the world. Something will survive us. Perhaps the rats will eventually take over and rebuild civilization. Perhaps, then, the rats will learn from our mistakes. But I very much hope we can rely on the leaders assembled here, and not on the rats.*» [15]

Nesta nova edição da «Cyberlaw by CIJIC», procuramos sustentar o crescimento paralelo que o Mestrado de Segurança da Informação e Direito do Ciberespaço[16] vai granjeando. É pois, com orgulho, que passaremos a destacar produção deste, com maior regularidade. Afinal, este é um desígnio da própria criação da revista. Provavelmente, num futuro não muito distante, estará na calha a edição em papel de futuras edições. Se há questão que se nos colocou com o teletrabalho foi: qual a redundância digital? *Ie*, sem acesso à internet, ou sem eletricidade/bateria, como é que seria possível aceder

14 «Não haverá normal: futuristas preveem mudanças permanentes pós-coronavírus», @ https://www.dn.pt/dinheiro/nao-havera-normal-futuristas-preveem-mudancas-permanentes-pos-coronavirus-11987179.html

15 Yuval Harari: «Yuval Harari's blistering warning to Davos», @ https://www.weforum.org/agenda/2020/01/yuval-hararis-warning-davos-speech-future-predications/

16 Mais informações @ : https://fenix.tecnico.ulisboa.pt/cursos/msidc

a conteúdos para efeitos de estudo? Como ler(aceder) nestas circunstâncias? Como mitigar a "info-exclusão" quando o sistema não é propriamente redundante na acessibilidade[17]?

Reavendo, nesta edição, incorporando conteúdo em inglês escrito, por força de deveres de participação, cooperação e colaboração internacional[18] que muito nos orgulha, procuramos revisitar temas como cibersegurança em contexto marítimo, dados pessoais e dados não pessoais, monitorização de trabalhadores em contexto laboral, a regulação jurídica do ciberespaço - mutação do paradigma à luz do acórdão James Elliot, *Phishing*, redes sociais e manipulação da opinião pública, o problema da mobilidade em contexto organizacional, e, os desafios da cibersegurança forense de *smartphones* no continente africano. Os temas são oportunos. São, igualmente, desafiantes. São, finalmente, abertos a colaboração múltipla, participada.

Resta-me agradecer a todos quantos contribuíram para mais uma edição da Revista, pelo esforço, pela disponibilidade, pela obra, endereçando a todos, em nome do Centro de Investigação Jurídica do Ciberespaço – CIJIC – da Faculdade de Direito da Universidade de Lisboa, um justíssimo: - Muito Obrigado.

Cyberlaw by CIJIC, ***Direito: a pensar tecnologicamente*.**

**Boas leituras.**

Lisboa, FDUL, 29 de Março de 2020

Nuno Teixeira Castro

17 Por exemplo, «Ministro Siza Vieira admite aulas por canais "estilo youtube" ou TV por cabo.», @ https://observador.pt/2020/03/29/ministro-siza-vieira-admite-aulas-por-canais-estilo-youtube-ou-tv-por-cabo/
Mas, sem acesso internet, ou sem cabo – até porque a cobertura não é de 100%, há, pelo menos, cerca de 20% de famílias sem acesso ao Cabo – como é que as crianças e adolescentes que se encontrem nesta situação se integram? Como é que se combate esta exclusão digital?
18 Um trabalho colaborativo ímpar. @ https://networkofcenters.net/center/cyberlaw-research-centre-university-lisbon-school-law-cijic


# DOUTRINA


# *THE MOBILITY PROBLEM IN ORGANIZATIONS*

**MARCO REIS** [1]

1 Master student in Information Security and Cyberspace Law in the University of Lisbon,IST and Lisbon Law School and Naval School of Portugal, 2019/2021.

## ABSTRACT

Since the early days of digital technology adoption that Organizations have been concerned with protecting their assets and information through physical and logical barriers, meant to prevent unauthorized accesses. These barriers were used to create a perimeter separating what is outside from the internal network. This concept was particularly successful at a time when most of the Organization's users were sitting inside the perimeter, and everyone else was outside.

However, current times have presented severe new challenges to the classic model. Generalized internet access, smartphones and Cloud services have enabled users to go mobile without losing computational capacity or connectivity. Critical services are offered from remote locations. Devices move off and on-premises seamlessly. It's all happening very fast, and there's little that can be done to prevent this without hampering business agility and progress. The perimeter, as we knew it, doesn't exist anymore, and the internal network is really wherever the users or assets happen to be.

My aim with this Paper is to analyze a few possible ways Organizations can broaden and/or complement their traditional perimeter protections, to better handle the new mobility challenges being faced today, and enable more adequate protection to their information, users and assets, wherever they may be.



**Keywords**: Technology; *Organizations; Networks and IT systems; Security and safety; Perimeter (new).*

# 1.INTRODUCTION

***"Thank you for coming.***
***We're going to make some history***
***together today."***

*Steve Jobs introducing the first iPhone on Jan. 9, 2007*

This is where it all started. Technology was finally sufficiently advanced to allow for an affordable device that offered, right in the palm of your hand, most of what computers were capable of. And cameras. And portable music players. And everything else developers could come up with trough the revolutionary app ecosystem.

Steve Jobs, the visionary that he was, recognized what this meant: mobility was about to move to the forefront of what technology was all about, and he was more than prepared to take the lead in a race that would shake up the industry, and leave most competitors either severely behind or in the dust[1] altogether.

1 (Hankin, 2019)

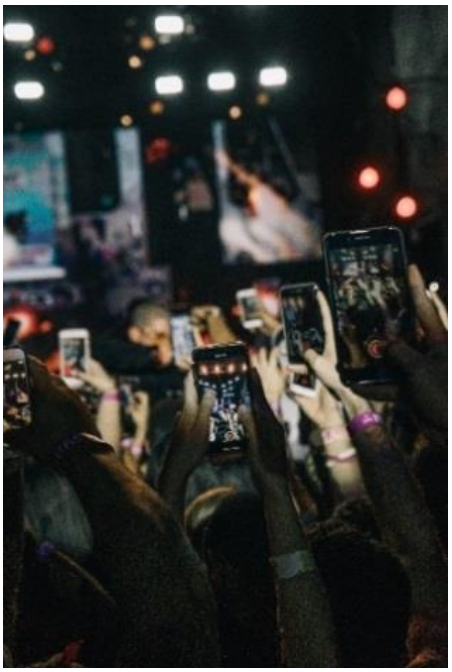

*Figure 1 - Crowd recording a live event with their smartphones*

The smartphone revolution[2] changed how people interacted with each other, consumed media, and used the internet. But it also changed **where** people did all these things.

2 (Molla, 2017)

## 2.PROBLEM STATEMENT

***"By 2020, over half of the employees will work remotely, but we still have not figured everything out to make this work"***

*Amir Salihefendic, CEO, Doist - The State of Remote Work in 2018*

Since starting to adopt technology long ago, Organizations have designed their Networks and IT systems with a Fort mentality. This typically means creating a perimeter, a set of barriers separating what is out from what is in, trying as much as possible to prevent any unwanted crossing of those barriers.

For a long time, this was very effective. Network and Systems were only accessible on- premises, and all the threats were kept out. Building a strong Fort was all that was needed.

Gradually, the slow but steady advance of technology started presenting additional challenges. The rise of the internet meant that a channel had to be created to interact with the outside from within. Such proposition proved impossible to resist, as there was simply too much value to be had from using the internet.

The solutions still seemed simple though. Content filtering started to be performed on the internet access, to try and prevent anything bad from coming in, or anything valuable from being sent out. Existing firewalls were improved so that more complex decisions could be made on what was allowed to cross the perimeter. But the truth of the matter was now evident: decisions were no long absolute but conditional. Organizations would have to start compensating by building and multiplying defense strategies, layering them together. Defense-in-depth[3] became a requirement.

3 (NIST, n.d.)

But not everything was bad. People still had to come to the office to access Organization resources. They still had the perimeter. Well, most of the time at least. Home internet access and Laptops became common, and suddenly it made sense that those devices should be allowed to work on company systems from the outside. The technology could support it, as Virtual Private Networks[4] (VPN's) could be used to extend the Network to the user location. They just had to be sure the anti-viruses were up to par on the endpoints.

And what about the Organizations they work with? Why shouldn't their most important partners share their network? It was just so convenient. No Organization operated alone anymore. Lower costs and higher agility and interoperability were there for the taking, at the cost of just a few more holes in the perimeter wall. They probably deployed Intrusion Prevention Systems[5] (IPS's) or some other now traditional perimeter defense commodities, just in case.

But then came the smartphones. Wi-Fi technology was now sufficiently developed as well. It was fast, it was reliable, and it was starting to appear everywhere. Not just in offices but at home, in shops and restaurants, hotels and shopping malls, airports and even airplanes. People started getting used to being online and connected all the time. They needed tools that they could use everywhere, and permanent access to the information they required.

Cloud services[6], a broader concept that also happens to enable internet-wide service, was the means through which all this could be achieved. And today it is already one of, if not the biggest business in technology. Because it is ideally poised to meet rising needs: the star sales lead needs it's critical business app while on the way to the next client meeting; the head of marketing needs a common platform to share files with the ad agency while waiting for his next flight; the finance controller is late and needs to connect to his scheduled monthly report meeting from his Uber to work. Everyone

4 (NIST, n.d.)
5 (NIST, n.d.)
6 (NIST, n.d.)

needs to do something, right now, no matter where from. That’s just the way things are done this day and age.

It's safe to say that the strategy needs to change.

## 3. CURRENT TRENDS

***"Longevity in this business is about being able to reinvent yourself or invent the future"***

*Satya Nadella, CEO at Microsoft*

Most historical companies in the information security space have recognized that their business model needs to change if they are to remain relevant at offering customers adequate means of protection, without hampering the ever-growing mobile workforce. And today a mobile workforce doesn't even necessarily mean that the employees work from home – although that trend is rapidly becoming the norm in many business models[7]. It may just mean that the employee has a smartphone and/or a laptop, and uses it to do additional work, planned or just because he can. After all, interacting with colleagues, customers or business partners can now be done at convenience.

On top of this, many new security companies have identified opportunities to disrupt the traditional players in this operating space, by offering more adequate and adjusted protection solutions to the mobile-first era, often leveraging cloud services and the as-a-service[8] model, that fit very well with internet focused strategies.

In most of these cases, the basic principles are the same: to replace the "border control" style approach with the idea that security must enforced where the users and information happen to be. And that trust must be earned. In other words, a "0-trust" model[9] approach where identity must be proven securely, and right of access dependent on pre-decided conditions.

These ideas are part of the fabric of Digital Transformation[10], which is a hot topic in today's world. Everyone recognizes the need for companies to adjust to these huge

7 (Buffer.com, 2019)
8 (Watts & Raza, 2019)
9 (Microsoft, 2019)
10 (Boulton, 2019)

changes brought on by very mobile and tech-savvy workforces and customer bases. Demands for flexibility, speed and service make time scarce to appropriately apply and enforce security, so it becomes critical to have the right strategy[11]. It must be adaptable to a much broader mix of use cases, and compatible with many different supporting infrastructure options, both internal and external.

After all, that transformation is very rarely immediate and sudden, which would have enormous costs and difficulties in migrating legacy systems, and systems with complex integrations and interfaces, all at once. On most medium and large companies that were already in operation this last decade, the most common scenario is a phased approach[12], where existing systems are gradually replaced with mobile-friendly and direct-to-cloud alternatives, or moved from on-premises to the cloud using "lift-and-shift" or other approaches[13], which doesn't really solve the legacy problem, but at least keeps companies moving in the right direction during a transition period that may take many years[14].

This naturally also applies to systems enforcing security. One can even make the case that changes to these systems need to be planned first, so that applications and data can be protected effectively once moved off-premises. If this move happens while you are still clinging to the appliances sitting in your data center, you're already too late.

11 (IBM, 2015)
12 (Kralj, 2017)
13 (Google Cloud, 2019)
14 (Ross, 2018)

## 4. THE NEW PERIMETER

***"We can leverage new identity standards to fill the gaps left by the disappearance of the traditional perimeter as we know it... the value now lies in using identity as the new perimeter."***

*John Hawke, Senior Director of Business Strategy at CA Technologies*

So, what remains unchanged with all these transformations happening, after abandoning your single, privately controlled infrastructure in favor of a hybrid or full cloud model?

Your users are still your users. And the company information is still your own.

Given the now public nature of access, Organizations just need to make sure that information is sufficiently protected at rest and in transit, and that identity management is performed at a level that offers adequate reliability and resilience. When you put it like this, it sounds simple. Because the nature of the problem is, in fact, easy to understand: everything is the same, but in different surroundings – both at the source of access, and at the destination.

Protecting information in transit usually means applying security to a significative number of different flows, like information being provided to and by stakeholders. E.g.: customers, suppliers, business partners, government entities; information uploaded or downloaded by employees; or interfaced systems exchanging information, either on-premises, in the cloud, or between both.

Doing the same for information at rest means protecting it while it is stored, be it in databases, disk storage, file sharing services, or user devices. Performing adequate identity management will be the way to make sure that only the intended and allowed

systems and users will be able to access and use the information during those stages, all the way through the information lifecycle up until it's secure deletion.

If Organizations make sure these protections are in place, then it shouldn't make a difference where systems and people physically are, and consequently the dependency on the perimeter for enforcing security is removed. Decision makers can start transitioning their businesses to a flexible model that is better prepared to serve their customers and will also make employees happier and more productive.

All this can be done without jeopardizing security. In fact, it can even possibly be increased in the process, because changes this transformational don't happen often at Organizations. It is usually the case that most on-premises systems and networks have been in place for a long time and don't have the ideal level of security in their design or implementation and may even be outdated due to lack of maintenance or support.

The most common scenario is that Organizations will have started with a baseline of network and core systems long ago, and have since spent their time adding new systems, building new features, gradually expanding their server and network base. Most replacements are only made out of necessity: either the requirements have changed and the current system is deemed obsolete or replaced; or the contract for a particular solution has reached its conclusion and the opportunity is taken to renew or replace the existing solution. This makes it so IT landscapes are much like the tree rings inside a tree: they are generally a product of how long Organizations have been in operation and are made up of different sections that have been put in place gradually over time. And because technology (and particularly security in technology) changed a lot over time, the "older rings" generally become liabilities.

Organizations can seize this opportunity and, with the right strategy[15] and architecture design, become much better prepared to deal with the new challenges of the present times.

15 (Brunswick & Olson, 2018)

It’s important to consider that enforcing security always comes at a cost. It may require extra investment, added complexity, reduced usability, or all of the above. This means that the user experience will probably be impacted when you increase your security posture. This may place you at odds with the initial intent of catering to your user base by enabling mobile access in the first place. That’s why it is so important, as is always the case when talking about security, to include communication and awareness initiatives in the project plan. People need to know what benefits they will get with the transformation initiatives, so that they will understand how adhere to the security requirements that come with them, and (ideally) even be glad to do so.

Designing the right processes, and choosing the right technology to support them, can mean the difference between successful projects and failed ones. That’s why an attempt to propose technical solutions to general problems must also be conceptual in nature.

In the context of this paper, a few types of solutions will be presented that may help Organizations achieve the recommended protection levels for mobile-first approaches. But, in reality, each Organization should begin its transformation journey with a deep understanding of the needs they must meet, the challenges to overcome, the characteristics of their business and people, and even their budget. And only then define the technological landscape that represents the best possible fit.

This being said, there are many types of solutions available in the market that aim to address the challenges presented in this paper. There are far too many of them to refer to individually, so the approach will be to try and refer a few of the more common and successful strategies that can be considered by all types of Organizations looking to address these same issues. And then offer examples of related tools that are available in the market with significant market penetration and success.

## 5. SECURING IDENTITY AND DEVICES

***"Given a choice between dancing pigs and security, users will pick dancing pigs every time."***

*Edward Felten, Deputy U.S. Chief Technology Officer*

Enforcing identity security will always impact the owner of the identity, which in most cases will mean a person that will either be an employee or customer. Sure, there are other cases, but they can all be handled as specific sub-sets to which the same underlying principles apply: the process of authentication must be strong and reliable, with a complete identity management process in place; the source must be secure and compliant with company policies; and usage should be within pre-approved parameters and scope.

We further establish these vectors with the following definitions:

- **Strong Authentication** is defined as method of proving identity that depends on verified proof of at least 2 of 3 factors: something the user knows (e.g. password); something the user has (e.g. his smartphone); and something the user is (e.g. biometrics).

- **Reliable Authentication** refers to the level of reliability and resilience inherent to the process of authentication and the tools involved, so that they can't be subverted. This may be assessed through testing the implemented processes and technical solutions for design flaws and vulnerabilities.

- **Identity Management** is the process through which the company manages its users at the three critical user lifecycle stages: provisioning, update and removal. The process should be auditable, synchronized with all companies' systems, and highly resilient to human mistakes (e.g. forgetting to decommission an employee's user after he leaves the company).

- **Device and User Security** is the level of protection offered to users and the devices they use to connect to company assets and access company information;
- **Acceptable Use** means a way to associate roles with identity, so that actions can specifically be allowed or disallowed depending on role. Successful actions should also be dependent on meeting sets of security criteria (e.g. if a user accesses a system while in Portugal in one minute, and coming from China the other, then something is wrong and the action should be blocked; if a user is human but is performing actions that only a computer could perform, then something is wrong and the action should be blocked; etc.).

The basic premise is that if Organizations can adhere to these concepts without either requiring the user to be on-premises or forcing him to use a VPN to connect to the internal network, then access can safely be granted from a roaming context.

Presented here are a few of the more relevant operating spaces, as defined by Gartner[16], where current technologies can be instrumental in helping Organizations to achieve these goals.

### 5.1 User Identity and Access Management

Gartner Definition: *"Identity and access management (IAM) (…) addresses the mission-critical need to ensure appropriate access to resources across increasingly heterogeneous technology environments, and to meet increasingly rigorous compliance requirements. IAM is a crucial undertaking for any enterprise. It is increasingly business-aligned, and it requires business skills, not just technical expertise. Enterprises that develop mature IAM capabilities can reduce their identity management costs and, more importantly, become significantly more agile in supporting new business initiatives."*

16 (Gartner, n.d.)

Solutions in this market seek to address the challenges related with authentication and identity management, usually providing the following set of base capabilities, among other more specific differentiators:

- **Strong, Multi-Factor Authentication:** secure authentication capabilities for your users from company devices or other sources, independent of location;
- **Single Sign-On:** improve usability by providing a single authentication step that proves identity, removing the need for additional authentication processes for corporate applications;
- **User Management, including Authorization, Application Access and Lifecycle:** manage complete identity process from a single central point, from initial provisioning to final decommission, including all role management and application access;

Examples:

- **OKTA**

https://www.okta.com/

*"Complete access management platform for your workforce and customers, securing all your critical resources from cloud to ground"*

- **PING IDENTITY**

https://www.pingidentity.com/en.html

*"Intelligent access for customers, employees and partners so they can securely connect to cloud, mobile, SaaS and on-premises applications and APIs"*

- **ONE LOGIN**

https://www.onelogin.com/

*"OneLogin delivers the unparalleled protection and control you need with the simplicity users demand, so you can get back to business"*

### 5.2 Endpoint Protection

Gartner Definition: *"An endpoint protection platform (EPP) is a solution deployed on endpoint devices to prevent file-based malware attacks, detect malicious*

*activity, and provide the investigation and remediation capabilities needed to respond to dynamic security incidents and alerts. (…) Desirable EPP solutions are primarily cloud-managed, allowing the continuous monitoring and collection of activity data, along with the ability to take remote remediation actions, whether the endpoint is on the corporate network or outside of the office. (…)".*

These solutions address some of the challenges related with securing the user and company devices. They represent an evolution from the traditional anti-virus solutions from the past, with the newer players in this space designed from the ground up to be particularly adjusted to a mobile focused user base and their devices, usually combining the following set of characteristics:

- **Cloud Based Protection:** security services are offered globally, independent of user and device location;
- **Next Generation Anti-Virus:** solutions don't only detect malware based on known signatures, but use a combination of specialized capabilities to detect and prevent unwanted behavior from unknown threats;
- **Flexible Agent:** endpoint agents are compatible with most relevant types of company assets, like smartphones, laptops, desktops, servers, and even virtual machines;

Examples:

- **CROWDSTRIKE**

https://www.crowdstrike.com/

*"Cloud-native endpoint protection platform built to stop breaches."*

- **CARBON BLACK**

https://www.carbonblack.com/

*"In today's mobile world, endpoints are the new perimeter (…) Carbon Black prevents more threats, gives you actionable insights, and helps you operate faster and more effectively"*

- **SENTINEL ONE**

https://www.sentinelone.com/

*"The end of antivirus. Our autonomous AI Platform defeats every attack, every second of every day. The number one antivirus replacement."*

### 5.3 Secure Web Gateway

Gartner Definition: *"(…) A secure Web gateway (SWG) is a solution that filters unwanted software/malware from user-initiated Web/Internet traffic and enforces corporate and regulatory policy compliance. These gateways must, at a minimum, include URL filtering, malicious-code detection and filtering, and application controls for popular Web-based applications, such as instant messaging (IM) and Skype. Native or integrated data leak prevention is also increasingly included."*

Far surpassing traditional proxies, the major players today can offer much more than just caching and content filtering for PC's on local internet access. Among the most popular capabilities are:

- **Content Filtering:** URL Filtering, Application Controls and Malware Detection over SSL Inspected Traffic;
- **Hybrid or Full Cloud Configurations:** in order to offer protection and policy enforcement to devices outside of the local network, local appliances can be combined with cloud services on some offerings to offer a Hybrid approach. Strictly cloud based solutions are also available;
- **Tamper-proof agents:** solutions will run agents on smartphones or laptops that will force internet traffic on those devices to be sent to the SWG from any location, acting like an always-on VPN client with added functionalities. Those agents will typically offer tamper-proof configurations so that, if defined by Organizational policy, protection and compliance can be enforced at all times;
- **Data Exfiltration Protection:** restrictions on service consumption (e.g. file sharing apps blocked), disallowed actions (e.g. block uploads) and several types of data loss prevention capabilities help Organizations protect against unwanted exfiltration of data.

Here are some of the major players today:

- **ZSCALER**

https://www.zscaler.com

*"With complete cloud security stack (...) you can deliver airtight security to all users, on or off network"*

- **SYMANTEC BLUECOAT**

https://www.symantec.com/products/secure-web-gateway

*"An advanced network security service that enforces consistent internet security and compliance policies for all users regardless of location or device."*

- **FORCEPOINT**

https://www.forcepoint.com/product/web-security

*"Next-generation web security for tomorrow's global workforce"*

## 6. CONCLUSION

***"It is not the strongest of the species that survives, nor the most intelligent that survives. It is the one that is the most adaptable to change"***

*Charles Darwin, English Naturalist and Geologist*

Most developed countries today are in a race to launch 5G[17]. This will offer higher internet speeds and lower latency for mobile devices, further increasing their capabilities and pushing even further the boundaries of what can be done remotely. The office, as we know it today, may soon become a thing of the past.

Organizations should embrace mobility as a key business critical capability, and re-design their security strategy accordingly. They will get a safer and more productive workforce, better protected assets and information, and a reinforced operational model that will be better adjusted to a new world that is already a reality.

As now commonly stated: *The perimeter is dead. Long live the (new) perimeter*.

17 (Cheng, 2019)

## BIBLIOGRAPHY


Boulton, C. (2019, May 31). *What is digital transformation? A necessary disruption*. Retrieved from cio.com: https://www.cio.com/article/3211428/what-is-digital-transformation-a-necessary-disruption.html

Brunswick, D., & Olson, J. (2018, September 27). *The Common-Sense Guide to IT Systems Modernization.* Retrieved from cleo.com: https://www.cleo.com/sites/default/files/2018-10/it-systems-modernization-guide.pdf

Buffer.com. (2019). *State of Remote Work Report*. Retrieved from https://buffer.com/state-of-remote-work-2019

Cheng, R. (2019, 10 27). *The 5G wireless revolution, explained*. Retrieved from cnet.com: https://www.cnet.com/news/the-5g-wireless-revolution-explained/

Deloitte. (2019). *Tech Trends 2019 - Beyond the Digital Frontier.* Retrieved from deloitte.com: https://www2.deloitte.com/content/dam/Deloitte/br/Documents/technology/DI_TechTrends2019.pdf

Gartner. (n.d.). *Gartner About Page*. Retrieved from gartner.com: https://www.gartner.com/en/about

Google Cloud. (2019, November). *CIO's Guide to Application Migration*. Retrieved from services.google.com: https://services.google.com/fh/files/misc/cio_guide_to_application_migraton.pdf

Hankin, A. (2019, 06 25). *Three Companies the iPhone Killed*. Retrieved from investopedia.com: https://www.investopedia.com/news/three-companies-iphone-killed/

IBM. (2015). *Increasing Agility and Speed to Drive Business Growth.* Retrieved from ibm.com: https://www.ibm.com/downloads/cas/PLOBJO7W

Kralj, M. (2017, November 1). *Cloud Migration: Finding your path to value with the cloud*. Retrieved from accenture.com: https://www.accenture.com/us-en/blogs/blog-miha-kralj-phased-approach-to-cloud-adoption

Microsoft. (2019). *Zero Trust Maturity Model.* Retrieved from microsoft.com: https://go.microsoft.com/fwlink/p/?linkid=2109181

Molla, R. (2017, 06 26). *How Apple's iPhone changed the world: 10 years in 10 charts*. Retrieved from vox.com: https://www.vox.com/2017/6/26/15821652/iphone-apple-10-year-anniversary-launch-mobile-stats-smart-phone-steve-jobs

NIST. (n.d.). *NIST Computer Security Resource Center - Glossary - Cloud Computing*. Retrieved from nist.gov: https://csrc.nist.gov/glossary/term/cloud-computing

NIST. (n.d.). *NIST Computer Security Resource Center - Glossary - Defense In Depth*. Retrieved from nist.gov: https://csrc.nist.gov/glossary/term/defense_in_depth

NIST. (n.d.). *NIST Computer Security Resource Center - Glossary - IPS*. Retrieved from nist.gov: https://csrc.nist.gov/glossary/term/intrusion-prevention-system

NIST. (n.d.). *NIST Computer Security Resource Center - Glossary - VPN*. Retrieved from nist.gov: https://csrc.nist.gov/glossary/term/VPN

Ross, J. (2018, April 5). *Digital Is About Speed — But It Takes a Long Time*. Retrieved from mit.edu: https://sloanreview.mit.edu/article/digital-is-about-speed-but-it-takes-a-long-time/

Watts, S., & Raza, M. (2019, June 15). *SaaS vs PaaS vs IaaS: What's the Difference and How to Choose*. Retrieved from bmc.com: https://blogs.bmc.com/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/?print=pdf