IV CURSO PÓS-GRADUADO EM BIOÉTICA
(18 DE JANEIRO A 7 DE JUNHO DE 2018)

UMA BREVE NOTA SOBRE OS DESAFIOS ÉTICOS DA *SAÚDE DIGITAL* ("*DIGITAL HEALTH*")

Miguel Patrício[1]

I. DEFINIÇÕES PRELIMINARES

A *saúde digital* ("*Digital Health*") é actualmente a expressão mais utilizada para englobar as tecnologias digitais aplicadas aos campos da medicina e da saúde.[2] Nesse sentido, não é substancialmente diferente da expressão "*e-health*" – a qual, nas palavras de Gunther Eysenbach[3], remete para "*an emerging field in the intersection of medical informatics, public health and business, referring to health services and information delivered or enhanced through the Internet and related technologies. In a broader sense, the term characterizes not only a technical development, but also a state-of-mind, a way of thinking, an attitude, and a commitment for networked, global thinking, to improve health care locally, regionally, and worldwide by using information and communication technology*."

O autor citado associa ao "*e-*" a (então nova) dimensão *electrónica* da medicina mas refere que há outros (10) "*e*"s que acompanham (ou devem acompanhar) essa nova dimensão:

[1] Professor da Faculdade de Direito da Universidade de Lisboa.
[2] Sobre a evolução destas tecnologias, e.g.: FRICKER, Samuel A.; THÜMMLER, Christoph; GAVRAS, Anastasius (Eds.) – *Requirements Engineering for Digital Health*. Basel, Springer, 2015, pp. 13 e ss..
[3] EYSENBACH, G. – "What is e-health?", in: *Journal of Medical Internet Research*, 3 (2) (e20), 2001.

"*efficiency*"; "*enhancing quality of care*"; "*evidence based*"; "*empowerment of consumers and patients*"; "*encouragement of a new relationship between the patient and health professional*"; "*education of physicians, through online sources, and consumers*"; "*enabling information exchange in a standardized way between health care establishments*"; "*extending the scope of health care*"; "*ethics*"; e "*equity*".

O leque das tecnologias digitais abarcado por estas expressões é amplo. P. ex., recorrendo ao elenco da agência norte-americana FDA, podemos estar a falar de: i) "*mobilidade em saúde*" ("*mobile health*" ou "*mHealth*"); ii) "*tecnologias de informação em saúde*" ("*health IT*"); iii) telesaúde e telemedicina; iv) *sensores e medidores de saúde*, seja sob a forma de adereços de vestuário ou implantes cutâneos ou subcutâneos ("*wearable healthcare devices*"); e de v) *medicina personalizada* (quando esta envolve dispositivos digitais colocados no interior dos pacientes para fins terapêuticos).[4]

É inquestionável que a grande maioria dos dispositivos munidos de tecnologias digitais (*smartphones, apps, fitness gadgets, assistentes cibernéticos*[5] – estejam ou não licenciados como aparelhos médicos) produzem dados... digitais, mas é

[4] Um dos primeiros autores a usar a expressão *saúde digital* foi Seth Frank, no artigo "Digital health care – the convergence of health care and the Internet" [in: *The Journal of Ambulatory Care Management*, 23 (2), 2000, pp. 8-17]. Nesse texto precursor, a *Internet* e a *Web* (com os seus *portais* e aplicações especializados) são consideradas factores impulsionadores de uma revolução no campo das *tecnologias de informação* em medicina, e nele se apontam, ainda, 5 vantagens para os pacientes, em resultado dos novos fluxos de informação: 1) dissemina-se informação; 2) auxilia à tomada de decisões informadas; 3) promove a saúde; 4) facilita a partilha de informação numa lógica de comunidade (conduzindo a uma gestão mais eficiente da mesma); 5) reduz o número (e, consequentemente, o custo) de serviços médicos desnecessários (ou que podem ser evitados com uma prevenção informada).

[5] É digna de nota a extraordinária evolução que se registou neste campo: em 1966, Alvan Feinstein (um dos "pais" da moderna epidemiologia clínica), numa recensão a um livro sobre "medicina cibernética", considerava impossível que os computadores pudessem vir a ter a capacidade de gerar nova informação e assegurava, de forma peremptória: "*a computer cannot do what we ourselves do not know how to do*." Será que hoje podemos dizer o mesmo?

necessário ter presente que também pode haver utilização de dados "analógicos" (que são convertidos em digitais) extraídos a partir de aparelhos que não são digitais (por ex., dados digitais criados a partir de informação extraída de aparelhos de diagnóstico sem capacidade de armazenamento de dados).

Decorre da observação que se fez a conclusão de que o campo da *saúde digital* envolve, mais do que aparelhos digitais, *processos digitais de obtenção e circulação de informação* (i.e., processamento digital de dados com respectivo tratamento em bases de dados para fins de análise por profissionais de saúde ou por terceiros). Dá-se o nome de "*big data*" biomédica ao (avassalador e intrincado) conjunto de informações que, neste contexto, se coligem e se analisam, seja à escala nacional ou internacional.

As vantagens do desenvolvimento destes sofisticados processos de circulação de dados biomédicos são evidentes e inquestionáveis: ajudar à monitorização do estado de saúde; promover hábitos saudáveis de actividade física ou de cumprimento rigoroso de terapias; reduzir custos/ineficiências, seja na prevenção ou nos tratamentos; aumentar a personalização das terapêuticas; contribuir para o aumento do ritmo de criação de novos fármacos e para o desenvolvimento da ciência médica.

É precisamente porque as vantagens são muitas e de monta, que existem riscos sérios de que, sem um correcto enquadramento no plano legal e ético, a *saúde digital* possa ficar ao serviço de interesses espúrios, sejam eles comerciais (um dos riscos mais tratados a este respeito é o da obtenção e manipulação de dados de saúde pessoais com intuitos comerciais) ou não.

II. DESAFIOS ÉTICOS DA *SAÚDE DIGITAL* ("*DIGITAL HEALTH*")

Nesta breve nota procurar-se-á elencar um conjunto de desafios com os quais se confronta a *saúde digital*, tendo sempre

presente que os mesmos tendem a multiplicar-se com o desenvolvimento cada vez mais acelerado da tecnologia nesta área específica. Para além de enunciar, de uma forma tópica, alguns dos desafios que se considera serem mais relevantes, procurar-se-á apontar para respostas aos mesmos – destacando, sempre que tal se justifique, as dimensões éticas a considerar (dado que a análise destas precede a construção de quaisquer eventuais "soluções" jurídicas).

> 1) A falta de representatividade das *amostras* (e até dos *universos*) das bases de dados digitais usadas para fins de desenvolvimento de produtos terapêuticos ou para a adopção de políticas públicas de saúde – uma falha que conduz ao enviesamento das conclusões que se retirem do tratamento estatístico feito.

Como resolver? Com a definição e harmonização dos "*standards*" de recolha e tratamento de dados estatísticos, sopesando, devidamente, a diversidade genética, etária, sexual ou socio-económica das populações abrangidas, entre outros factores; em casos mais complexos, fazendo uso, p. ex., de *amostras de referência* para fins de comparação com os resultados que venham a ser obtidos.

A maior minúcia de análise, através da afinação daqueles "*standards*", permitirá, sem dúvida, o avanço da *medicina de precisão* ("*precision medicine*").[6] Um avanço que poderá, contudo, ser minado pela possibilidade de, em determinados Estados, se limitar o acesso às bases de dados, ou impor condições cientifica ou eticamente injustificadas à partilha das mesmas com terceiros Estados (ou centros de investigação internacionais).

Note-se que os desafios em torno da recolha e gestão dos

[6] Embora também haja quem mostre reservas quanto aos caminhos que a mesma pode tomar. Vd., por ex., PRAINSACK, Barbara – "Personhood and solidarity: what kind of personalized medicine do we want?", in: *Personalized Medicine*, 11 (7), 2014, pp. 651-657; MCGONIGLE, Ian V. – "The collective nature of personalized medicine", in: *Genetic Research*, 98 (e3), 2016.

dados vão além desta questão estatística. Como bem sintetiza Christine Aicardi *et alii* (2016)[7], há outros cinco grandes desafios a resolver: 1) o conceito de "informação pessoal" está a atravessar uma actualização tecnológica, uma vez que a protecção da mesma abarca agora bem mais intervenientes do que o *binómio* médico-paciente; 2) a total anonimização dos dados pessoais é (quase) impossível (sendo que, em casos como os da investigação biomédica, pode ser indesejável tanto para investigadores como para participantes); 3) a informação dada ao paciente, para que este consinta (ou não) o uso futuro dos seus dados pessoais, deve ser completa e clara, ainda que o modo como se fará uso da mesma no futuro possa passar por processos hoje desconhecidos (o paciente deve, pelo menos, ter a consciência dessa incerteza); 4) uma blindagem da informação recolhida em contexto médico é vital para que esta não passe para domínios (nomeadamente comerciais) não pretendidos pelo paciente (e a recolha de dados a partir de dispositivos que não explicitam essa finalidade como, e.g., *apps* ou *fitness gadgets* que, em tempo real, recolhem dados pessoais sobre a actividade dos seus utilizadores, faz crescer a preocupação...); 5) a forma como os dados recolhidos serão utilizados para estabelecer inferências em estudos de *análise preditiva* – visto que os erros, falhas ou omissões relevantes na informação disponibilizada (ou na forma como a mesma é tratada) passam indetectados ao paciente e este dificilmente terá oportunidade de as descobrir e rectificar ou, até, de evitar que as mesmas possam ser – pelo menos em tese – utilizadas contra si...).

> 2) O risco de deixar as referidas tarefas de tratamento de dados (nomeadamente o estabelecimento de correlações) a componentes dotados de (imprevisível) "*inteligência artificial*" ou a anónimos (mas

[7] Vd. AICARDI, Christine *et alii* – "Emerging ethical issues regarding digital health data. On the World Medical Association Draft Declaration on Ethical Considerations Regarding Health Databases and Biobanks", in: *Croatian Medical Journal*, 57 (2), 2016, p. 208.

não inofensivos...) algoritmos de computação, sem haver, neste contexto, um democrático e exigente escrutínio (prévio e independente) dos mesmos (esta questão poderá também aplicar-se à introdução de novos dispositivos médicos[8]).

Como resolver? Como é evidente, é de admitir a utilização de tais componentes ou algoritmos... mas desde que submetidos ao referido escrutínio – o que isto significa, por outras palavras, é que, mesmo naqueles casos em que as correlações de dados, assim estabelecidas, pareçam "robustas" aos olhos dos investigadores, a prática frequente de testes à fiabilidade dos resultados é uma condição essencial para se poder confirmar ou infirmar tais ligações – assim se garantindo a segurança clínica de novos tratamentos ou fármacos, ou de eventuais novas políticas públicas de saúde a implementar.

3) A questão da protecção da privacidade e da segurança dos dados pessoais em saúde, agora exponenciada à escala digital e agravada pela incapacidade dos mecanismos tradicionais – como os da "anonimização" (dada a possibilidade de reconstrução de dados por via de "*hacking*") ou do "consentimento prévio" (dado que as listas de utilizações possíveis dos dados deixam sempre de fora hipóteses nem sequer imaginadas por clientes, pacientes ou *cobaias* de testes clínicos) – para travar utilizações abusivas.

Como resolver? Reforço de mecanismos legais de protecção de dados pessoais, garantindo que o consentimento é precedido de explicações claras e detalhadas sobre o que pode ser

[8] Veja-se o caso (que, apesar de antigo, é muito citado) das máquinas de radioterapia *Therac-25* (1985-7). Sobre este caso, ver, e.g.: LEVESON, Nancy G. *et alii* – "An investigation of the Therac-25 accidents", in: *Computer*, 26 (7), 1993, pp. 18-41; MACQUAID, Patricia A. – "Software disasters – understanding the past to improve the future", in: *Journal of Software: Evolution and Process*, 24 (5), 2012, pp. 459-470; BIRSCH, Douglas – "Moral responsibility for harm caused by computer system failures", in: *Ethics and Information Technology*, 6 (4), 2004, pp. 233-245.

disponibilizado (e a quem); e, também, um reforço da monitorização e da vigilância dos sistemas de segurança dos dados, com eventual agravamento das penas (pecuniárias ou outras) devidas em caso de violação das regras de utilização dos dados pessoais.

Ainda assim, a constante evolução das tecnologias (e, em especial, dos *sistemas de informação*) obrigará as entidades públicas a terem de realizar esforços permanentes na implementação, na prática, daqueles mecanismos legais. Por outro lado, a legislação também terá de ser capaz de definir, com a necessária prudência (atendendo aos valores e interesses em potencial conflito), as fronteiras do "*direito à não-partilha*".[9]

Talvez menos evidente mas igualmente importante seja a necessidade de criação de *mecanismos de confiança* para acesso a certos dados pessoais. Por ex.: demonstrar a transparência dos métodos usados; informar da existência de meios de responsabilização (civil, penal, disciplinar) potencialmente aplicáveis aos detentores dos dados; provar que a partilha desses dados traz mais resultados benéficos do que prejudiciais; identificar e "vigiar" os futuros detentores da informação (e, se estes forem "meras" máquinas, saber quem é o proprietário delas – ou quem é que delas pode extrair vantagens económicas); por fim, criar mecanismos de responsabilização para os referidos vigilantes.

O recente Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho, de 27/4/2016, sobre protecção de dados pessoais (que substitui a Directiva 95/46/EC a partir de 25/5/2018) acentua, acertadamente: a importância da "minimização dos dados" pessoais ("*data minimisation*") e do direito de oposição ao "*profiling*" (i.e., a qualquer forma automatizada de processamento de informação pessoal, com o objetivo de avaliar e tipificar os indivíduos com base nos seus dados pessoais) por

[9] Neste contexto, não poderá ser ignorada a dimensão etnográfica da questão, dado que, como refere Bob Simpson, "[there are] *culturally specific versions of how people conceive of relationality, duty, care and the obligations they feel they owe to others*." ["A «we» problem for bioethics and the social sciences: a response to Barbara Prainsack", in: *Science, Technology, and Human Values*, 43 (1), 2018, p. 45].

parte dos titulares dos dados; a necessidade de "pseudonimização" ("*pseudonimization*")[10]; e, em particular, a exigência do consentimento explícito para o processamento de dados pessoais. Contudo, também se reconhece que tal consentimento nem sempre será possível (por ex., no caso de dados obtidos num projecto de investigação científica serem partilhados para uso em outros projectos) – nomeadamente, se tal projecto de investigação visar solucionar um problema de *interesse público*, um problema premente de *saúde pública* (excepção que, ainda assim, pode não aplicar-se, por exemplo, à informação genética, se determinado Estado entender que esta deve beneficiar de uma protecção reforçada).[11]

Às escalas nacionais, é, ainda, necessário assegurar que as múltiplas disposições relativas à protecção dos dados pessoais (regras constitucionais, legais, regulamentares, civis, penais ou administrativas) convergem para a definição de um regime legal claro e apto a permitir responsabilizar, na área da investigação, os intervenientes na cadeia de circulação ou partilha de dados

[10] Apesar destas cautelas, basta ler, por exemplo, estes artigos para ficar com uma ideia mais clara (e mais assustadora) acerca das possibilidades de re-identificação de informações anonimizadas: LUBARSKY, Boris – "Re-identification of «anonymized data»", in: *Georgetown Law Technology Review*, 1 (1), 2016, pp. 202-213; ROTHSTEIN, Mark A. – "Is deidentification sufficient to protect health privacy in research?", in: *The American Journal of Bioethics*, 10 (9), 2010, pp. 3-11. A prova prática das referidas possibilidades foi feita há mais de 20 anos, numa experiência realizada por Latanya Sweeney em 1997...

[11] A definição do que é "*interesse público*", para os fins do disposto no Regulamento, também pode gerar dúvidas. Como referem RUMBOLD, John Mark Michael; PIERSCIONEK, Barbara – "The effect of the General Data Protection Regulation on medical research", in: *Journal of Medical Internet Research*, 19 (2) (e47), 2017: "*The derogations for research without consent have been expanded to specifically include medical research where «in the public interest» (Recital 51). How public interest will be defined has not been elaborated, but European jurisprudence demands member states satisfy a high threshold where human rights are involved (eg, a «pressing social need»). This standard would not be required for the conduct of medical research using databanks, but it might exclude all commercial research for «me too» drug development (drugs that offer no advantages over drugs already on the market), arrangements that have no evidence of benefit sharing, or simply require that projects address issues of public importance regardless of the profits made*."

biomédicos digitais – criando-se, assim, as bases para a harmonização dos regimes de protecção de dados entre países comunitários.[12]

> 4) A questão da partilha de dados biomédicos pessoais através de dispositivos digitais (habitualmente não licenciados como dispositivos médicos) para fins comerciais (declarados ou encapotados). Com efeito, crescentemente surgem no mercado *apps* com (alegadas) finalidades *desportivas* (ou até "*médicas*") – as "*sensor network apps*"[13] –, através das quais os consumidores/utilizadores podem estar a facultar e partilhar em rede informações pessoais sobre rotinas, localização, hábitos alimentares ou de exercício físico, e até sobre maleitas.[14]

---

[12] No mesmo sentido, CHASSANG, Gauthier – "The impact of the EU general data protection regulation on scientific research", in: *Ecancer Medical Science*, 11 (709), 2017, a p. 11: "*Research participants, as data subjects, have several rights allowing them to maintain a certain degree of control over their personal data processed in the course of the research. While there was hope for achieving a new level of harmonisation on this topic, the GDPR is quite deceiving as, even if it fixes new important rights of general application such as the right to be forgotten or the right to data portability, they could not apply in the field of research, if the EU or member States laws provides, under certain conditions, legitimate exceptions, as it is stated under Article 89. This situation is mainly due to an absence of conferred competency to the EU to harmonise legislations in the field of health and scientific research, the EU having only a support competency in these fields remaining principally regulated by national laws. This results in the incapacity for the EU to adopt fully harmonised rules through EU law without the formal agreement of EU Member States, this explaining the limited content of Article 89 that fixes rules depending on the state of the art of national or EU laws. Thus, Member States should provide for appropriate safeguards for the processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes*."

[13] Sobre as múltiplas modalidades possíveis de "*sensor networks*" na área da saúde, v., e.g.: AL AMEEN, Moshaddique; LIU, Jingwei; KWAK, Kyungsup – "Security and privacy issues in wireless sensor networks for healthcare applications", in: *Journal of Medical Systems*, 36 (1), 2012, pp. 93-101.

[14] Um estudo recente de Achilleas Papageorgiou *et alii* ("Security and privacy analysis of mobile health applications: the alarming state of practice", in: *IEEE Access*, 6, 2018, pp. 9390-9403), que envolveu a análise de 24405 *apps* ligadas à area da saúde, para sistemas *iOS* (21953) e *Android* (2452), revelou alguns dados preocupantes: "*the*

Como resolver? Se os produtos digitais licenciados estão sujeitos a avaliação prévia de idoneidade e cumprimento das regras de protecção de dados pessoais, já estas *apps* (mas também a *social networking* ou os *fitness gadgets*) colocam sérios desafios: porque se situam numa "*zona cinzenta*", dando, por vezes, a entender que são aparelhos médicos (ou algo próximo); porque podem extrair informação pessoal de consumidores sob formas desconhecidas (apesar da – mas também por causa da – rápida aceitação de longas e por vezes crípticas "*licenças de utilização*" pedidas na instalação de programas ou na entrada em *redes sociais*); enfim, porque poucos serão os utilizadores que exigem saber, em detalhe, a *política de privacidade* (i.e., disponibilização de dados) adoptada.

Acresce, ainda, como dificuldade adicional, que estes produtos são muitas vezes vendidos apenas por via "*web*" – podendo, deste modo, escapar a *filtros* fronteiriços no Estado do comprador (sendo que a informação cedida poderá, também, ser facultada a terceiros sem obedecer às exigências legais que possam existir nesse Estado).

---

results showed that 95.63% of the apps pose at least some potential damage through information security and privacy infringements, whereas 11.67% of them estimated to impose the highest potential damages" (p. 9392); "*Our experiments showed that 80% of the analyzed apps transmit users' health-related data, while 20% store them locally on the device. In terms of security, only 50% of those apps transmit health-related data over HTTPS connections for all of their communication.*" (p. 9395); "*20% of the apps ask users to submit personal photo*" (*ibidem*); "*35% of the apps transmitted users' geolocation information or their postal address either to their vendors or to third parties.*" (p. 9396); "*While all the apps transmitting search queries send them to their vendor's domain, 80% of them send this information to third parties as well, and two apps send their users' queries to 16 different third party domains.*" (*ibidem*). Estes autores assinalam, também, que o "*GDPR specifies in broad terms the types of data included in the definition of «data concerning health», and only substantially increases what is specified in the* [*predecessor*] *DPD.*" Assim sendo, e na sequência dos esforços desenvolvidos pelo *Article 29 Working Party*, caberá, agora, ao *European Data Protection Board* (EDPB), na vigência do novo Regulamento, estabelecer e afinar, de forma detalhada, os limites e as finalidades admissíveis para o uso da denominada "*health data*" (que, sendo maior do que "*medical data*", pode ser, ou não, considerada "*personal data*" para fins de protecção legal) – nomeadamente a que é gerada a partir de *apps* e dispositivos digitais móveis.

Perante tamanhas dificuldades, apenas a regulamentação harmonizada das regras entre Estados e, por outro lado, uma mais clara separação e identificação dos mercados (*produtos médicos* vs. *produtos não-médicos*), acompanhada de uma eficaz vigilância e recriminação de "publicidades duvidosas" – que, ou visam conferir uma *capa médica* a produtos puramente comerciais, ou dissimular a dimensão ou subvalorizar a importância dos dados pessoais que podem vir a ser partilhados com terceiros –, permitirá responder, de uma forma satisfatória, aos desafios que estes novos dispositivos, hoje em dia cada vez mais disseminados, nos colocam.[15]

Ainda neste contexto, não será de excluir a possibilidade de criação de processos de certificação específicos para dispositivos digitais ou *apps* (com finalidade médica ou não), considerando os fluxos de informação por estes solicitados, gerados, organizados e partilhados. A fiscalização destes fluxos é essencial e urgente, dado que, na prática, se tem assistido à gradual diluição das divisões que se aplicavam à forma como os dados pessoais eram tratados e colocados ao serviço de objectivos comerciais, terapêuticos ou de investigação médica.[16]

---

[15] Um estudo (detalhado) sobre o impacto, vantagens e desvantagens dos chamados "*wearable sensors*" pode ser visto, por ex., em: SCHUKAT, Michael *et alii* – "Unintended consequences of wearable sensor use in healthcare", in: *Yearbook of Medical Informatics*, 1, 2016, pp. 73-86.

[16] Como notam, com acerto, Christine Aicardi *et alii*, em "Emerging ethical issues regarding digital health data. On the World Medical Association Draft Declaration on Ethical Considerations Regarding Health Databases and Biobanks", in: *Croatian Medical Journal*, 57 (2), 2016, a p. 211: "*It must furthermore be noted that the boundaries between health care, commercial, and research purposes are increasingly blurred. This is evidenced, for example, by the fact that a private company selling personal genomics services (23andMe) received NIH funding to build survey tools, expand its gene database, and use its stores of genetic data for research projects. Another example is that a philanthropic foundation established a $20 million endowment at Harvard Business School «to find ways to accelerate breakthroughs and advance commercialization of precision medicine by harnessing the energy and ideas of the medical, science and entrepreneurial communities in the city». More easily than ever before, data generated for one kind of purpose and services (eg, marketing) can be repurposed for other kinds of projects and services (eg, health and social care).*"

> 5) O risco de "*hacking*" dos dispositivos. Como se não bastassem os riscos de um potencial uso abusivo dos dados pessoais por parte dos comercializadores daqueles aparelhos e *apps* (como se viu, *maxime*, no ponto *4)*, também existe o sério risco de que, pela via digital, *absolutos desconhecidos* tenham acesso àqueles dados. Neste contexto, assume particular relevância (porque é mais apelativo para os "*hackers*") o acesso indevido a bases de dados em saúde (às informações que, naturalmente, não são de acesso livre) e aos *biobancos*.[17]

Como resolver? Também aqui se pode dizer, tal como sucedia quanto a alguns dos pontos anteriormente analisados, que já existem regras internacionais (e, em muitos casos, nacionais) que visam o combate ao "*hacking*" (embora não directamente o tipo de "*hacking*" aqui tratado). É o caso, e.g., da Convenção de Budapeste sobre o cibercrime.

Contudo, como bem se assinala num estudo da autoria de Mirja Gutheil *et alii*, encomendado pela Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos (LIBE) do Parlamento Europeu[18], "*the Budapest Convention is based on the*

---

[17] Neste contexto, Guy Martin *et alii* ("Cybersecurity and healthcare: how safe are we?", in: *BMJ*, 358, 2017, p. 2) identificam sete potenciais ameaças cibernéticas: "[1] *Data theft for financial gain – stealing personal data for the purposes of monetary gain; for example, names, addresses, social security details, financial information*; [2] *Data theft for impact – theft and public release of sensitive medical information; for example, celebrities, politicians, or other high profile people*; [3] *Ransomware – using malware to block users from their data or systems or to delete data unless a fee is paid*; [4] *Data corruption – deliberate corruption of data, such as altering test results, for political or personal gain*; [5] *Denial of service attacks – disruption of a network or system by flooding it with superfluous requests, motivated by blackmail, revenge, or activism*; [6] *Business email compromise – creating fake personal communications for financial gain; for example, obtaining fraudulent payments or personal information*; [7] *The unwitting insider – substantial disruption to systems or the loss of data owing to the unintentional actions of staff using outdated and at-risk systems*."

[18] GUTHEIL, Mirja *et alii – Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices*. Brussels, European

assumption that the physical location of the data is known. Given the nature of the internet, the expansion of cloud computing services and the fact that these services and channels are owned and controlled by private international companies, many services are provided across borders. Therefore, law enforcement agencies may not know in which country, or even continent, certain data reside – this has resulted in the concept of «loss of location», as termed in the Council of Europe paper, or more precisely, «loss of knowledge of location». In fact, in the case of cloud computing, even the service provider might not know where such data are located. […]. *The traditional law enforcement response to such instances would be to seek cooperation with the other country through procedures for mutual legal assistance, as governed by the 2000 Convention on Mutual Assistance in Criminal Matters between the Member States of the EU, which uses as its basis the European Convention on Mutual Assistance in Criminal Matters (CoE, 12.06.1959). However, mutual assistance procedures are deemed to be «cumbersome or ineffective». Given the ease with which such data can be moved with high frequency, alongside the difficulties identifying the location of such data, this assessment of mutual assistance is particularly true when law enforcement agencies are seeking digital evidence*."

Também a chamada Declaração de Taipé de 2002 ["*World Medical Association Declaration of Taipei on Ethical Considerations regarding Health Databases and Biobanks*"], revista pela última vez em 2016, não deixa de ser um bom instrumento para a correcta *governação* destas bases de dados mas, infelizmente, não contém respostas ou propostas para o combate a intrusões de terceiros. E esta é uma questão maior porque, desde empresas multinacionais farmacêuticas (e outras com interesse comercial directo) até organizações (ou Estados)

Parliament, Policy Department for Citizens' Rights and Constitutional Affairs, 2017, p. 28.

terroristas ("*bio-terroristas*"), muitos são os que podem querer aproveitar-se (preferencialmente, de forma anónima) dos dados armazenados.

No espaço da UE, não se poderá esquecer o quadro legislativo que actualmente existe, nomeadamente o art. 16.º do Tratado sobre o Funcionamento da União Europeia, os artigos 7.º, 8.º e 11.º da Carta dos Direitos Fundamentais da União Europeia, o já referido Regulamento Geral sobre a Proteção de Dados [Regulamento (EU) 2016/679], a Directiva 2002/58/EC [que se espera que seja substituída, em 2019, pelo Regulamento da Privacidade das Comunicações Electrónicas (Regulamento *ePrivacy*)], ou a Directiva 2013/40/UE relativa a ataques contra os sistemas de informação.

Contudo, à escala mundial, sabendo-se que existem Estados que não têm sequer (uma mínima) legislação relativa ao "*hacking*" (e, muito menos, ao "*hacking*" que possa envolver dispositivos médicos ou de saúde), resta apelar à harmonização de "*standards*" (seja no plano dos níveis de segurança a aplicar às bases, seja no reforço da cooperação entre as entidades policiais e judiciais dos diferentes Estados), uma vez que a mesma é a condição essencial para prevenir e impedir intrusões, descobrir a origem das que foram bem sucedidas e responsabilizar os seus autores.

> 6) Os desafios do "*registo clínico electrónico*" ("*Electronic Health Record*"). As vantagens obtidas com este tipo de registo são evidentes, mas os problemas também devem ser assinalados, como, e.g.: como garantir a confidencialidade e a segurança[19], ou a *interoperacionalidade* fronteiriça dos registos[20]? Quem deve ser o titular (e o responsável

[19] Por ex., face a um potencial uso, por parte de *biobancos*, dos dados desses registos: v. CAENAZZO, L.; TOZZO, P.; BOROVECKI, A. – "Ethical governance in biobanks linked to electronic health records", in: *European Review for Medical and Pharmacological Sciences*, 19 (21), 2015, pp. 4182-6.

[20] Como refere, a este respeito e no contexto da UE, André den Exter ["eHealth law:

último) por tais registos? Como evitar a redução dos (já de si diminutos) tempos médios das consultas em resultado da necessidade de preenchimento de documentação electrónica?[21] A montante destas questões, como combater a iliteracia digital de certas populações?[22]

Como resolver? No espaço comunitário, a solução deve passar pela criação, de raiz, de um quadro legislativo que harmonize o que, actualmente, não tem ido além da "manta retalhada" dos normativos nacionais (cada qual espelhando a sua sensibilidade própria para as questões referidas).[23]

No que diz respeito, especificamente, à iliteracia digital, é justo reconhecer que existem (e são úteis) projectos

---

The final frontier?", in: HERVEY, Tamara K.; YOUNG, Calum Alasdair; BISHOP, Louise E. (Eds.) – *Research Handbook on EU Health Law and Policy*. Cheltenham, Edward Elgar Publishing, 2017, p. 247]: "*Aimed at solving the missing interoperability of electronic health systems and limited data exchange, the eHealth network of national authorities formulated guidelines on the standardization of patient summary records to be exchanged across borders*. [...]. *But standardization alone is insufficient to remove all barriers to cross-border data exchange. The legal requirement of cross-border interoperability of national EHR laws or systems is largely absent in most Member States but crucial for the cooperation and cross-border exchange of health data*."

[21] Genericamente, a respeito das questões éticas que estes registos podem colocar, veja-se, p. ex.: OZAIR, Fouzia F. *et alii* – "Ethical issues in electronic health records: A general overview", in: *Perspectives in Clinical Research*, 6 (2), 2015, pp. 73-6; DYER, Kirsti A. – "Ethical challenges of Medicine and health on the internet: A review", in: *Journal of Medical Internet Research*, 3 (2) (e23), 2001; SPRIGGS, Merle *et alii* – "Ethical questions must be considered for electronic health records", in: *Journal of Medical Ethics*, 38, 2012, pp. 535-539.

[22] A este respeito, ver, por exemplo: WITTEN, N. A.; HUMPHRY, J. – "The electronic health literacy and utilization of technology for health in a remote Hawaiian community: Lana'i", in: *Hawai'i Journal of Medicine & Public Health*, 77 (3), 2018, pp. 51-59; TIEU, Lina *et alii* – "Online patient websites for electronic health record access among vulnerable populations: portals to nowhere?", in: *Journal of the American Medical Informatics Association*, 24 (e1), 2017.

[23] E não é apenas nesta área específica da *saúde digital*: por ex., também na área da telemedicina falta um quadro legislativo uniforme à escala comunitária [vd. RAPOSO, Vera Lúcia – "Telemedicine: The legal framework (or the lack of it) in Europe", in: *GMS Health Technology Assessment*, 12, 2016, 12 p.].

comunitários como o "*IC-Health – Improving digital health literacy in Europe*", que é suportado pelo Programa-Quadro *Horizonte 2020*, e que visa a criação de "*35 open access online courses (MOOCs), in seven different national languages, for different population cohorts*". Pena é que este projecto (que tem o seu término previsto para este ano) seja o único actualmente financiado pela UE ao abrigo do programa "*SC1-HCO-12-2016 – Digital health literacy*"...

> 7) As "armadilhas" da auto-medicação e da auto-terapia por via de dispositivos e informações digitais. Devem os cidadãos passar a ser produtores e detentores exclusivos da sua informação médica? Poderão eles confiar em *sites* pseudo-médicos? Não correrão o risco de exacerbar, por "excesso" de informação, a reacção a "sintomas" que têm (ou que julgam ter)?[24] Poderão eles possuir um *boletim clínico* (pessoal) mais detalhado do que o do médico de família? Num outro plano, devem os cidadãos poder ter acesso, mesmo sendo saudáveis, a *técnicas de «melhoramento bio-tecnológico»* (ditas "*trans-humanistas*")[25] que podem ser executadas no recato da casa de cada um (por ex.: implantação de *chips* ou sensores, ingestão de nano-partículas, uso de *próteses inteligentes*)?

Como resolver? A montante, é necessária uma maior ligação entre o ensino e a prática da medicina e estas novas

[24] STARCEVIC, Vladan – "Cyberchondria: Challenges of problematic online searches for health-related information", in: *Psychoteraphy and Psychosomatics*, 86, 2017, pp. 129-133; AIKEN, Mary – "The age of cyberchondria", in: *RCSIsmj Review*, 5 (1), 2012, pp. 71-74.

[25] A este respeito, e.g.: DEL AGUILA; Jorge W. Vásquez; SOLANA, Elena Postigo – "Transhumanism, neuroethics and human person", in: *Revista Bioética*, 23 (3), 2015, pp. 503-510. Considerando o "*trans-humanismo*" uma espécie de "*new riff on the old eugenics tune*", vd.: KOCH, Tom – "Enhancing who? Enhancing what? Ethics, Bioethics, and Transhumanism", in: *Journal of Medicine and Philosophy*, 35 (6), 2010, pp. 685-699.

realidades tecnológicas (que ou são desconhecidas ou subvalorizadas por uma parte da comunidade médica). É também importante o aumento da pedagogia dos médicos junto da sociedade civil visando desincentivar as práticas da auto-medicação e da auto-terapia[26]; e tal não dispensa, naturalmente, a regulamentação, clara e restritiva, sobre a utilização desses dispositivos e "*técnicas*", bem como, se tal se afigurar viável, sobre o acesso aos mesmos através da "*web*".

REFERÊNCIAS BIBLIOGRÁFICAS

AICARDI, Christine *et alii* – "Emerging ethical issues regarding digital health data. On the World Medical Association Draft Declaration on Ethical Considerations Regarding Health Databases and Biobanks", in: *Croatian Medical Journal*, 57 (2), 2016, pp. 207-213.

AIKEN, Mary – "The age of cyberchondria", in: *RCSIsmj Review*, 5 (1), 2012, pp. 71-74.

AL AMEEN, Moshaddique; LIU, Jingwei; KWAK, Kyungsup – "Security and privacy issues in wireless sensor networks for healthcare applications", in: *Journal of Medical Systems*, 36 (1), 2012, pp. 93-101.

BENNADI, Darshana – "Self-medication: A current challenge", in: *Journal of Basic and Clinical Pharmacy*, 5 (1), Dec. 2013/Feb. 2014, pp. 19-23.

BIRSCH, Douglas – "Moral responsibility for harm caused by computer system failures", in: *Ethics and Information Technology*, 6 (4), 2004, pp. 233-245.

CAENAZZO, L.; TOZZO, P.; BOROVECKI, A. – "Ethical

[26] Vd. BENNADI, Darshana – "Self-medication: A current challenge", in: *Journal of Basic and Clinical Pharmacy*, 5 (1), Dec. 2013/Feb. 2014, pp. 19-23.

governance in biobanks linked to electronic health records", in: *European Review for Medical and Pharmacological Sciences*, 19 (21), 2015, pp. 4182-6.

CHASSANG, Gauthier – "The impact of the EU general data protection regulation on scientific research", in: *Ecancer Medical Science*, 11 (709), 2017, pp. 1-12.

DEL AGUILA; Jorge W. Vásquez; SOLANA, Elena Postigo – "Transhumanism, neuroethics and human person", in: *Revista Bioética*, 23 (3), 2015, pp. 503-510.

DYER, Kirsti A. – "Ethical challenges of Medicine and health on the internet: A review", in: *Journal of Medical Internet Research*, 3 (2) (e23), 2001.

EXTER, André den – "eHealth law: The final frontier?", in: HERVEY, Tamara K.; YOUNG, Calum Alasdair; BISHOP, Louise E. (Eds.) – *Research Handbook on EU Health Law and Policy*. Cheltenham, Edward Elgar Publishing, 2017, pp. 242-263.

EYSENBACH, G. – "What is e-health?", in: *Journal of Medical Internet Research*, 3 (2) (e20), 2001.

FEINSTEIN, Alvan – "*Cybernetic Medicine* [*book review*]", in: *Yale Journal of Biology and Medicine*, 38 (4), 1966, pp. 381-382.

FRANK, Seth – "Digital health care – the convergence of health care and the Internet", in: *The Journal of Ambulatory Care Management*, 23 (2), 2000, pp. 8-17.

FRICKER, Samuel A.; THÜMMLER, Christoph; GAVRAS, Anastasius (Eds.) – *Requirements Engineering for Digital Health*. Basel, Springer, 2015.

GUTHEIL, Mirja *et alii* – *Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices*. Brussels, European Parliament, Policy Department for Citizens' Rights and Constitutional Affairs, 2017.

KOCH, Tom – "Enhancing who? Enhancing what? Ethics,

Bioethics, and Transhumanism", in: *Journal of Medicine and Philosophy*, 35 (6), 2010, pp. 685-699.

LEVESON, Nancy G. *et alii* – "An investigation of the Therac-25 accidents", in: *Computer*, 26 (7), 1993, pp. 18-41.

LUBARSKY, Boris – "Re-identification of «anonymized data»", in: *Georgetown Law Technology Review*, 1 (1), 2016, pp. 202-213.

MACQUAID, Patricia A. – "Software disasters – understanding the past to improve the future", in: *Journal of Software: Evolution and Process*, 24 (5), 2012, pp. 459-470.

MARTIN, Guy *et alii* – "Cybersecurity and healthcare: how safe are we?", in: *BMJ*, 358, 2017, pp. 1-4.

MCGONIGLE, Ian V. – "The collective nature of personalized medicine", in: *Genetic Research*, 98 (e3), 2016.

OZAIR, Fouzia F. *et alii* – "Ethical issues in electronic health records: A general overview", in: *Perspectives in Clinical Research*, 6 (2), 2015, pp. 73-76.

PAPAGEORGIOU, Achilleas *et alii* – "Security and privacy analysis of mobile health applications: the alarming state of practice", in: *IEEE Access*, 6, 2018, pp. 9390-9403.

PRAINSACK, Barbara – "Personhood and solidarity: what kind of personalized medicine do we want?", in: *Personalized Medicine*, 11 (7), 2014, pp. 651-657.

RAPOSO, Vera Lúcia – "Telemedicine: The legal framework (or the lack of it) in Europe", in: *GMS Health Technology Assessment*, 12, 2016, 12 p..

ROTHSTEIN, Mark A. – "Is deidentification sufficient to protect health privacy in research?", in: *The American Journal of Bioethics*, 10 (9), 2010, pp. 3-11.

RUMBOLD, John Mark Michael; PIERSCIONEK, Barbara – "The effect of the General Data Protection Regulation on medical research", in: *Journal of Medical Internet Research*, 19 (2) (e47), 2017.

SCHUKAT, Michael *et alii* – "Unintended consequences of

wearable sensor use in healthcare", in: *Yearbook of Medical Informatics*, 1, 2016, pp. 73-86.

SIMPSON, Bob – "A «we» problem for bioethics and the social sciences: a response to Barbara Prainsack", in: *Science, Technology, and Human Values*, 43 (1), 2018, pp. 45-55.

SPRIGGS, Merle *et alii* – "Ethical questions must be considered for electronic health records", in: *Journal of Medical Ethics*, 38, 2012, pp. 535-539.

STARCEVIC, Vladan – "Cyberchondria: Challenges of problematic online searches for health-related information", in: *Psychoteraphy and Psychosomatics*, 86, 2017, pp. 129-133.

TIEU, Lina *et alii* – "Online patient websites for electronic health record access among vulnerable populations: portals to nowhere?", in: *Journal of the American Medical Informatics Association*, 24 (e1), 2017.

WITTEN, N. A.; HUMPHRY, J. – "The electronic health literacy and utilization of technology for health in a remote Hawaiian community: Lana'i", in: *Hawai'i Journal of Medicine & Public Health*, 77 (3), 2018, pp. 51-59.