Research Directions: Quantum Technologies

www.cambridge.org/qut

Developing a human rights compatible governance framework for quantum computing

Ot van Daalen

Faculty of Law, Instituut voor Informatierecht, Amsterdam, Netherlands

Impact Paper

Cite this article: van Daalen O (2024). Developing a human rights compatible governance framework for quantum computing. *Research Directions: Quantum Technologies*. **2**, e1, 1–6. https://doi.org/10.1017/qut.2024.2

Received: 9 January 2024
Accepted: 26 February 2024

Keywords
quantum computing; human rights; governance

Corresponding author:
Ot van Daalen; Email: o.l.vandaalen@uva.nl

Abstract

Quantum computers hold significant promise for peaceful applications, but one of the more immediate potential applications is breaking of public key encryption technologies. This poses significant risks to the information security of global digital infrastructure in a broader sense. At the same time, the development of quantum computing is a quintessentially scientific undertaking. There is a tension in the scientific freedom required to develop these technologies, and the measures to mitigate the risks associated with quantum computers. Policy for resolving this tension must be in line with the human right to science, read together with the right to privacy and the right to freedom of expression. In this article, I apply these rights to the development of quantum computing to provide guidance for government policy on quantum computing. I conclude that states must create the conditions for scientific research to flourish, even if this research may carry significant societal risks. This applies also to research and development of quantum technologies. In the context of quantum computing, this primarily means investing in the development and uptake of alternative encryption technologies which are resistant to attacks by quantum computers. It also means regulating the use of these technologies for applications which are undesirable.

Introduction[1]

Quantum computing is a multi-purpose technology. Quantum computers hold significant promise for peaceful applications, in domains such as logistics, finance and medicine. But one of the more immediate potential applications, should quantum computers become sufficiently powerful, is the breaking of public key encryption technologies. That's an application which is mostly useful for governments in their intelligence gathering activities, activities which are strongly related to the military domain. It's also an application which poses significant risks to the information security of global digital infrastructure in a broader sense. Given the potential risks of this technology, it makes sense to determine which policies – rules or otherwise – are needed to shape the development of quantum computing.

One simplified way of determining these rules, is by balancing the opportunities associated with these technologies with the risks. But this assessment is complicated by the fact that the development of quantum computing is a quintessentially scientific undertaking: getting these machines to work at scale requires an intricate understanding of physical effects at quantum level, combined with technologies which can sense and manipulate reality at that level. Insights from this research may lead to spin-offs which have little to do with quantum technologies, and with benefits that are difficult to calculate. Moreover, the development of science very much depends on the freedom of scientists, to choose what to focus on, to collaborate and to share knowledge.

There's an obvious tension in the scientific freedom required to develop these technologies, and the measures which may be contemplated to mitigate the risks associated with quantum computers. For example, quantum computer-related export controls could limit the risks posed to digital infrastructure, but these measures also impact international collaboration. One important question is how this tension can be resolved when devising policy on quantum computing. I explore this in this article.

One aspect of this answer lies in the application of the human right to science, read together with the right to privacy and the right to freedom of expression. In this article, I apply these rights to the development of quantum computing to provide guidance for government policy on quantum computing. First, I shortly discuss quantum computing, the risks of breaking public key encryption and the scientific nature of the development of this technology. Then I discuss the human rights framework, focusing on the European Convention for Human Rights (the Convention), the European Union Charter of Fundamental Rights (the Charter) and the Covenant on Economic, Social and Cultural Rights (the Covenant). Finally, I then apply this framework to the development of quantum computing, and draw lessons for other contexts.

[1]Elements of this work are part of a PhD which was defended in October 2022 (van Daalen, 2022).

Research Directions

CAMBRIDGE UNIVERSITY PRESS

The main answer to the question is that the right to science, read together with the right to privacy and the right to freedom of expression, imposes on governments' two obligations. First, states must create the conditions for scientific research to flourish, even if this research may carry significant societal risks. This applies also to research and development of quantum technologies. But states must at the same time take measures to mitigate the risks involved in these activities. This sometimes means developing "counter"-technologies. In the context of quantum computing, this primarily means investing in the development and uptake of alternative encryption technologies which are resistant to attacks by quantum computers. It also means regulating the use of these technologies for applications which are undesirable.[2]

Quantum computing is a multi-purpose technology, which can also break public key encryption

Quantum computers have long remained a theoretical possibility envisioned by scientists, not a thing which actually works. But even when these technologies were still vapourware, experts agreed that *if* it worked, it could be used for a number of applications. Feynman in the eighties of the last century suggested that it could be used to simulate physics.[3] Since this would allow for much more efficient chemical engineering, it could lead to breakthroughs in medicine, fertilisers, batteries.[4] The other potential use lies more in the realm of mathematics, namely to compute discrete logarithms and factoring. This could be used in domains such as finance and logistics.[5]

And one concrete application of quantum computers in this domain is the breaking of public key encryption. This is based on an invention of an algorithm by mathematician Peter Shor in 1994.[6] This algorithm makes it possible to quickly calculate the private encryption key on the basis of a public key, if the quantum computer has a sufficient size, something which is currently impossible with classical computers. The breaking of public key encryption is one of the main reasons why governments are investing much time and resources into the development of quantum computers. The inventor of the keybreaking algorithm, Shor, even predicted that "[i]f the only uses of quantum computation remain discrete logarithms and factoring, it will likely become a special-purpose technique whose only raison d'être is to thwart public key cryptosystems."[7]

Still, the impact of breaking public key encryption technologies with quantum computers does not immediately lead to the world's information becoming transparent to everyone with an internet connection. Most importantly, only a select few will initially have access to a sufficiently powerful quantum computer, if only because there will be very few working quantum computers at first. Given the primary application of these computers – namely codebreaking – it is likely that these will include governments. A government can own the computer directly, for example if it was developed by the intelligence agency, or, if it was developed by a private company, it can enlist the computer for these purposes.

Having access to these machines is, however, not enough: you also need access to the information which you want to decrypt. This means you will have to be able to intercept communications flowing over the internet (or other networks), or access information stored on servers (to the extent that these are encrypted with public key encryption technologies). Again, these physical capabilities are often limited to governments. We know for example from the Snowden revelations that the United States and the United Kingdom have far-reaching access to messages transmitted via undersea cables landing at their shores – but its fair to expect that many others have the legal and technical capabilities in place to intercept communications flowing through their territory.[8]

Finally, especially in the beginning, quantum computers will speed up the recovery of private keys from public keys, but decryption will not be so fast so as to make it instantaneous (this could become different when these computers grow even more powerful, allowing the near-instant decryption of large sets of keys).[9] So at first, governments will have to focus on a limited set of information which they will want to encrypt.

After this initial phase, however, there will come a time when access to these computers will be broadened. It is possible that remote, shared access to quantum computers will also become available. When that happens, others will also be able to use this information to start breaking public key encryption. Again, this also presupposes access to the encrypted information, but one can imagine that others than governments, such as organised crime, or commercial entities trying to gain an economic advantage, may in fact be able to gain access to some information – for example by intercepting communications over the air locally, by breaking into the infrastructure of communications service providers or by gaining unauthorised access to encrypted data on servers (which in some cases may also be encrypted with public key encryption).

So when quantum computers become sufficiently powerful, we will have to contend with the realistic possibility that some of the information currently encrypted with public key technologies can be decrypted by governments and private parties. This in itself is already highly problematic for the persons and institutions whose data would be subject to attacks – one could imagine for example diplomatic traffic between governments and their embassies becoming available to other countries, which has the potential to upset diplomatic relations or even worse outcome. But a more fundamental effect of this, is that it will affect trust in digital infrastructure: for users of digital infrastructure, it will become difficult to assess whether particular information may be decrypted at will by attackers, which may affect the use of this infrastructure. For my analysis, it is not necessary to further determine the extent of these risks: it is already sufficient to establish that the development of a powerful quantum computer will in the foreseeable future have negative impact on the confidentiality of information and the trust in digital infrastructure.

The rights to science, freedom of expression and privacy

The question then is how this relates to the rights to science, freedom of expression and privacy. The rights to science and freedom of expression, viewed from an abstract level, serve the

[2]van Daalen (2022).

[3]Feynman (1982, 1986).

[4]See e.g. Hoofnagle and Garfinkel (2021), Budde and Volz (2019), Evers et al. (2021), Choi (2021) and Choi (2022).

[5]See for an overview, e.g., Herman et al. (2023).

[6]Shor (1994, 1997). As as sidenote, another algorithm was developed around that time which could also speed up the breaking of symmetric algorithms, but the efficiency gains are not as spectacular, and the impact is therefore deemed to be limited, so this will receive no further attention in this contribution.

[7]Shor (1994, 1997).

[8]MacAskill et al. (2013).

[9]Engineering National Academies of Sciences [2018].

https://doi.org/10.1017/qut.2024.2 Published online by Cambridge University Press

same goals, roughly related to safeguarding the access, analysis and sharing of information in the public interest. The right to privacy serves in part the interest of ensuring the confidentiality of information, and, read together with freedom of expression, the confidentiality of communications. The challenge is to find an appropriate balance between these interests within the legal framework.

The right to science and the right to freedom of expression

The right to science, read together with the right to freedom of expression, not only protects the right to perform scientific research, and share the results of this – it also imposes on states a duty to mitigate the harmful effects of science. I have expanded on this further in another article in the context of information security.[10] I will provide a short summary of this argument here.

For purposes of this article, three instruments relating to the right to science are relevant.[11] In 1948, it was recognised in Article 27 of the Universal Declaration of Human Rights (the Declaration).[12] In 1966, it was adopted in Article 15 of the International Covenant on Economic and Social Rights (the Covenant), which protects the right to "enjoy the benefits of scientific progress and its applications." And finally, the right is protected under the European Charter of Fundamental Rights in Article 13, which considers that the "arts and scientific research shall be free of constraint" and that "academic freedom shall be respected."

Under the Covenant, the right to science is primarily informed by four documents. Firstly, there's the Venice Statement, developed between 2007 and 2009 by human rights experts, which set the stage, by highlighting the obligation of states to respect scientific freedom while preventing the misuse of science and technology that could impede human rights and fundamental freedoms.[13] This balance is suggested to be achieved through legal and policy frameworks that promote the development and diffusion of science and technology in a way that is consistent with fundamental human rights, as well as by promoting nondiscriminatory access to the benefits of science and its applications.[14]

In a 2012 report, Special Rapporteur Farida Shaheed then further stressed the link between the right to science and the freedom of expression, advocating for the freedom of inquiry and the importance of freely sharing scientific research.[15] She points to the positive impact of scientific progress on people's well-being and human rights, while also highlighting the need for protection against the harmful applications of science.[16]

UNESCO then developed this further in 2017, by recommending that researchers operate in a spirit of intellectual freedom, encouraging states to facilitate the publication and access to scientific knowledge, while ensuring that any restrictions are minimal and subject to safeguards.[17]

And finally, the Committee on Economic, Social and Cultural Rights (CESCR) in 2020, through its General Comment on the right to science, emphasised the necessity of robust protection for research freedom, considering it essential to determine the research's direction and method and to share results.[18] It advocates for prioritising the development of science for peace and human rights and highlights the importance of the precautionary principle to avoid harm when full scientific certainty is lacking, suggesting that public deliberation is key in balancing the interests of scientific freedom with potential risks.[19] The CESCR also acknowledges the profound implications of scientific and technological advancements, such as quantum computers, on the enjoyment of rights, urging states to enact policies that enhance benefits while mitigating risks and to engage in global cooperation to manage these risks effectively.[20]

Article 13 of the Charter should be understood as building on this edifice. The explanatory memorandum states that this right is deduced primarily from the right to freedom of thought and expression, to be exercised having regard to Article 1 (on human dignity) and subject to the limitations under Article 10 of the Convention.[21] But of course the considerations from the Covenant equally apply in the context of the Charter.

Finally, the right to freedom of expression as laid down in Article 10 of the Convention and Article 11 of the Charter further supports the right to science, but there are a number of things which distinguishes it in a subtle way. First, it emphasises the informational aspects of the scientific process – it protects the access to, and sharing of "information and ideas." Second, it attaches a lot of weight to the public interest aspects of this information.[22] Finally, Article 10 of the Convention explicitly imposes duties and responsibilities on the beneficiaries of these rights, which implies a certain duty of care on researchers to limit and mitigate potential damage.[23]

The right to privacy

So while the right to science, read together with the right to freedom of expression, not only imposes on states an obligation to protect the development of science, it also imposes on states an obligation to mitigate the related risks. One of the main risks of the research and development of quantum computers, as outlined above, is that of breaking public key cryptography and affecting trust in digital infrastructure.

This also leads to the question how this risk mitigation obligation relates to the right to privacy. This is a relevant question, because the right to privacy, read together with the right to freedom of expression, protects confidentiality – of private information and of communications. One way to ensure this confidentiality, is through the application of encryption technologies, exactly the application which could be undermined by sufficiently advanced quantum computers.

I have analysed the relationship between encryption technologies and the right to privacy (and data protection) in another

[10]van Daalen (2022).

[11]See for literature on the right to science; Mann et al. (2020), Smith (2020), Mann and Schmid (2018), Morgera (2015), Butenschon Skre and Eide (2013), Gran et al. (2013), Donders (2011), Müller (2010), Shaver (2009), Schabas (2007); see for an early analysis of scientific freedom (Zoontjens, 1993).

[12]Universal Declaration of Human Rights [1948].

[13]UNESCO (2009).

[14]UNESCO (2009), art. 16(a) and (b).

[15]Shaheed (2019), par. 18 and 21.

[16]Shaheed (2019), par. 24 and recommendation (m).

[17]UNESCO (2017), par. 16, 38.

[18]CESCR (2020), par. 13.

[19]CESCR (2020), par. 6, 22, 57.

[20]CESCR (2020), par. 74–76, 81.

[21]Explanations Relating to the Charter of Fundamental Rights [2007].

[22]See for example *Magyar Helsinki Bizottság v Hungary* [2016], par. 162.

[23]*Stankiewicz and others v Poland* [2014], par. 62; see before *Bladet Tromsø and Stensaas v Norway* [1999], par. 65; *Fressoz and Roire v France* [1999], par. 54; *Steel and Morris v United Kingdom* [2005], par. 90.

https://doi.org/10.1017/qut.2024.2 Published online by Cambridge University Press

article in-depth.[24] There, I conclude that when it comes to governmental measures relating to encryption, the risk of unlawful access to private information and confidential communication is central to the determination of an interference and the assessment of proportionality. For purposes of this article, I will provide only a short outline of the analysis under Article 8 of the Convention and Article 7 of the Charter (which protects the right privacy) and Article 8 (which protects the right to data protection).

Firstly, for the right to privacy to apply under both instruments, there must be an "interference." The challenge is that developments that impact encryption technologies, may weaken the effectiveness of confidentiality measures, but this does not necessarily mean that states will also gain access to information. The Court has, however, dealt with this challenge, in cases involving secret surveillance and the storage of personal data, recognising that the fear and chilling effect of surveillance, as well as the mere storage of personal data, can already constitute interferences.[25] In cases of secret surveillance, the Court has acknowledged that the fear of being spied upon, can itself be an interference with privacy rights. Similarly, the Court has held that the storage of personal data, such as DNA profiles and fingerprints, is an interference due to the potential future uses of this data. Restrictions that facilitate lawful access or increase the risk of unlawful access to private can have chilling effects on behaviour. Given this analysis, I contend that measures facilitating lawful access to private information, as well as those significantly increasing the risk of unlawful access, should be considered interferences with privacy and freedom of expression.

The next question is how this interference should be assessed under these provisions. Both the ECHR and the CJEU focus on protecting individuals from arbitrary interference and abuse of power by public authorities.[26] This involves distinguishing between lawful and unlawful access to information, with the former being evaluated under negative obligations (preventing state interference) and the latter under positive obligations (addressing non-state actors' interference). The Courts have established criteria for lawful state surveillance, emphasising the need for clear, detailed rules to avoid arbitrariness. These rules should specify the conditions and limits of surveillance, including the nature of offenses justifying surveillance, categories of people surveilled, duration limits, data handling procedures, and conditions for data erasure or destruction.

In general, the Courts conduct a balancing exercise to assess surveillance measures, weighing the government's justification against the potential for abuse. This includes examining the nature, scope, and duration of measures, the grounds for ordering them, the authorities involved, and available remedies. The margin of appreciation varies depending on the aim, such as national security. In this analysis, the risk of unlawful surveillance is also a key concern. The ECHR acknowledges that technology can increase this risk, particularly with advanced surveillance capabilities and direct access to communications by security services.[27] Information security measures can also decrease the risk of abuse.[28] The ECHR has also noted the importance of secure data storage, restricted data disclosure, and detailed logging in surveillance operations to minimise the risk of unlawful access.[29]

The ECHR further recognises states' positive obligations under Article 8 to protect individuals from unlawful access by private parties. This includes ensuring effective legal safeguards, particularly for sensitive data like medical records.[30] This means states must provide practical and effective protection to prevent unauthorised access. This is important, because it directly relates to the risk-mitigating measures which governments are expected to take in the face of a potential breakdown of current public key cryptography infrastructure as more advanced quantum computers will become available.

Applying this framework to the governance of quantum computing

Taking the three human rights discussed above as the basis for a broader framework shaping the governance measures of states in the field of quantum computing, the following can be concluded. First, the scientific nature of the domain of quantum computing is highly dependent on global collaboration for sharing and developing knowledge. This makes it important for talent and resources to be shared and used across borders. The documents on the right to science discussed above make clear that states should be very reluctant in applying controls on global exchange of knowledge in this field.

In particular, in view of the risks of quantum computing, the application of export controls requires an evaluation of controls on a case-by-case basis. These controls currently require an authorisation process for exports, considering the end-use, end-user, and the human rights record of the importing country. This process doesn't outright prohibit exports, but places a responsibility on governments to judiciously evaluate the potential applications of quantum technologies. The balance to be struck is delicate: promoting scientific progress while safeguarding against technologies being used in ways that could contravene human rights interests. One factor which is relevant is the way in which the importing government may use the knowledge to decrypt information contrary to internationally applicable human rights requirements. Where this appears likely, an export license should be denied.

But of course, there will always remain the risk of states building and deploying quantum computers, even in the face of export controls. This means that states also have an obligation to mitigate the risks of decryption by investing in the development and deployment of protective technologies, in particular post-quantum cryptography. This means not only supporting the scientific development of these technologies through funding, but also making sure that the uptake of this technologies goes sufficiently quickly, investing in awareness campaigns and clarifying that security standards also require the implementation of PQC algorithms. I also recommend governments keeping track of progress on the PQC transition through annual reports. This is particularly important in view of the risk that encrypted data may be collected now by adversaries – when it cannot yet be decrypted – and will be stored for decryption later, when quantum computers have become sufficiently advanced.

The other aspect which follows from the above framework, is the use of quantum computers for decryption purposes. Because

[24]van Daalen (2023).

[25]See *Roman Zakharov v Russia* [2015]; *S and Marper v United Kingdom* [2008]; *Digital Rights Ireland and others* [2014]; *La Quadrature du Net* [2020].

[26]See *Roman Zakharov v. Russia* [2015] (n 25); *Digital Rights Ireland and others* [2014] (n 25).

[27]*Szabó and Vissy v Hungary* [2016], par. 73, 79.

[28]*Big Brother Watch and others v United Kingdom (Grand Chamber)* [2021], par. 362.

[29]*Centrum för Rättvisa v Sweden (Grand Chamber)* [2021], par. 311–316.

[30]*I v Finland* [2008], par. 38.

https://doi.org/10.1017/qut.2024.2 Published online by Cambridge University Press

governments have a positive obligation to minimise unlawful access to private information by third parties, this means they have to adopt a robust framework around the use of these technologies for these goals. In particular, decryption using quantum computers by private parties should only be allowed in specific cases, such as to retrieve a lost private key (e.g. when someone lost the password to their encrypted communications). This will have to be enforced via technological and contractual means. There are very few other situations in which the use of a quantum computer by private parties to decrypt information should be allowed. Private parties should for example be prohibited from reconstructing private keys from intercepted public keys. Whether these restrictions can be enforced is an interesting topic for further research, though.

Furthermore, the conditions under which governments themselves may resort to quantum decryption are equally important. I contend that the right to privacy and freedom of expression does not stand in the way of governments in certain cases using quantum computers to decrypt communications. But in order to respect the rights of privacy and freedom of expression, the law must prescribe well-defined conditions for such application in order to avoid abuse of this power. This approach must aim at preventing arbitrary or unjustified interference, thereby maintaining a balance between national security and the rights to privacy and freedom of expression. Given the difficulty of knowing in advance what the content of the communications will be, such decryption operations should be surrounded by the strictest safeguards. This means that they must be strictly targeted at specific communications, and that prior supervision of these decryption powers by a court is imperative. And the key pairs generated during quantum decryption processes must be securely deleted post-use to prevent potential theft or misuse.

Finally, states have a responsibility in ensuring that advancements in quantum computing are leveraged for the benefit of humanity. This includes the imperative to share the results of government-funded research openly and without discrimination. Whether an obligation to disseminate this knowledge could also extend to the results of research conducted by private parties is more complicated, in view of the rights to property (including intellectual property) and the freedom to conduct a business. This is also a relevant topic for further exploration.

Data availability statement. This contribution is not based on the analysis of data.

Author contribution. This contribution has been written by O.L. van Daalen.

Financial support. This work was supported by the Netherlands Organisation for Scientific Research (NWO), as part of the Quantum Software Consortium programme (project number 024.003.037/3368).

Competing interests. The author declares not conflict of interest.

Ethics statement. Ethical approval and consent are not relevant to this article type.

Connections references

D'Auria, V., & Teller, M. (2023). What are the priorities and the points to be addressed by a legal framework for quantum technologies? *Research Directions: Quantum Technologies*, **1**, E9. https://doi.org/10.1017/qut.2023.3.

References

Budde F and Volz D (2019) Quantum computing and the chemical industry. *McKinsey & Company*, July 12. Available at https://www.mckinsey.com/industries/chemicals/our-insights/the-next-big-thing-quantum-computings-potential-impact-on-chemicals (accessed 19 December 2023).

Butenschon Skre A and Eide A (2013) The Human right to benefit from advances in science and promotion of openly accessible publications. *Nordic Journal of Human Rights* **427**. Available at https://heinonline.org/HOL/P?h=hein.journals/norjhur31&i=429 (accessed 20 September 2019).

CESCR (2020) General Comment No. 25 (2020) on Science and Economic, Social and Cultural Rights (Article 15 (1) (B), (2), (3) and (4) of the International Covenant on Economic, Social and Cultural Rights), United Nations. E/C.12/GC/25.

Choi CQ (2021) Quantum computing makes inroads towards pharma. *IEEE Spectrum*, March 2. Available at https://spectrum.ieee.org/quantum-drug (accessed 19 December 2023).

Choi CQ (2022) How quantum computers can make batteries better. *IEEE Spectrum*, January 20. Available at https://spectrum.ieee.org/lithium-air-battery-quantum-computing (accessed 19 December 2023).

Donders Y (2011) The right to enjoy the benefits of scientific progress: In search of state obligations in relation to health. *Medicine, Health Care and Philosophy* **14**, 371–381.https://doi.org/10.1007/s11019-011-9327-y.

Engineering National Academies of Sciences (2018) Quantum Computing: Progress and Prospects. Available at https://www.nap.edu/catalog/25196/quantum-computing-progress-and-prospects (accessed 21 August 2020).

Evers M, Heid A and Ostojic I (2021) Quantum computing in drug development. *McKinsey & Company*, June 18. https://www.mckinsey.com/industries/life-sciences/our-insights/pharmas-digital-rx-quantum-computing-in-drug-research-and-development (accessed 19 December 2023).

Feynman RP (1982) Simulating physics with computers. *International Journal of Theoretical Physics*, **21**, 467–488. https://doi.org/10.1007/BF02650179.

Feynman RP (1986) Quantum mechanical computers. *Foundations of Physics* **16**, 507–531. https://doi.org/10.1007/BF01886518.

Gran B, Waltz M and Renzhofer H (2013) A child's right to enjoy benefits of scientific progress and its applications. *The International Journal of Children's Rights* **21**, 323–344.https://doi.org/10.1163/15718182-02102002.

Herman D, *et al.* (2023) Quantum computing for finance. Nature Reviews Physics 5, 450–465. http://arxiv.org/abs/2307.11230.

Hoofnagle CJ and Garfinkel S (2021) *Law and Policy for the Quantum Age*. 1st Edn, Cambridge University Press.

MacAskill E, *et al.* (2013) GCHQ taps fibre-optic cables for secret access to world's communications. *The Guardian*, June 21. Available at http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa (accessed 16 September 2020).

Mann SP, Porsdam H and Donders Y (2020) 'Sleeping beauty': The right to science as a global ethical discourse. *Human Rights Quarterly* **42**, 332–356. http://muse.jhu.edu/article/754939.

Mann SP and Schmid MM (2018) Health research priority setting: State obligations and the human right to science. *The American Journal of Bioethics* **18**, 33–35 https://doi.org/10.1080/15265161.2018.1523492.

Morgera E (2015) Fair and equitable benefit-sharing at the cross-roads of the human right to science and international biodiversity law. *Laws* **4**, 803–831. https://www.mdpi.com/2075-471X/4/4/803.

Müller A (2010) Remarks on the Venice statement on the right to enjoy the benefits of scientific progress and its applications (Article 15(1)(b) ICESCR). *Human Rights Law Review* **10**, 765–784. https://academic.oup.com/hrlr/article/10/4/765/782653.

Schabas W (2007) Study of the right to enjoy the benefits of scientific and technological progress and its applications. In Donders Y and Volodin V (eds.), *Human Rights in Education, Science, and Culture: Legal Developments and Challenges*. Ashgate Publishing, Ltd.

Shaheed F (2019) The right to enjoy the benefits of scientific progress and its applications. Available at https://primarysources.brillonline.com/browse/human-rights-documents-online/promotion-and-protection-of-all-human-rights-civil-political-economic-social-and-cultural-rights-including-the-right-to-development;hrdhrd99702016149 (accessed 1 October 2019).

Shaver L (2009) The right to science and culture. Wisconsin Law Review 2010, 121–184. https://papers.ssrn.com/abstract=1354788.

Shor PW (1994) Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*. Available at https://ieeexplore.ieee.org/document/365700 (accessed 19 December 2023).

Shor PW (1997) Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing 26, 1484. http://arxiv.org/abs/quant-ph/9508027.

Smith T (2020) "Understanding the nature and scope of the right to science through the travaux préparatoires of the universal declaration of human rights and the international covenant on economic, social and cultural rights. The International Journal of Human Rights 24, 1156–1179. https://doi.org/10.1080/13642987.2020.1715947.

UNESCO (2009) The right to enjoy the benefits of scientific progress and its applications. *Experts' Meeting*. Available at https://unesdoc.unesco.org/ark:/48223/pf0000185558 (accessed 20 September 2019).

UNESCO (2017) *Recommendation on Science and Scientific Researchers*. UNESCO.

van Daalen O (2022) In defense of offense: Information security research under the right to science. *Computer Law & Security Review* **46**, 105706. https://linkinghub.elsevier.com/retrieve/pii/S026736492200053X.

van Daalen OL (2022) *Making and Breaking with Science and Conscience: The Human Rights-Compatibility of Information Security Governance in the Context of Quantum Computing and Encryption*. Van Daalen Press.

van Daalen OL (2023) The right to encryption: Privacy as preventing unlawful access. *Computer Law & Security Review* **49**, 105804. https://www.sciencedirect.com/science/article/pii/S0267364923000146.

Zoontjens PJJ (1993) *Vrijheid van Wetenschap: Juridische Beschouwingen over Wetenschapsbeleid En Hoger Onderwijs*. WEJ Tjeenk Willink.

Big Brother Watch and others v United Kingdom (Grand Chamber) [2021] ECHR Applications nos. 58170/13, 62322/14 and 24960/15.

Bladet Tromsø and Stensaas v Norway [1999] ECHR Application no. 21980/93.

Centrum för Rättvisa v Sweden (Grand Chamber) [2021] ECHR Application no. 35252/08.

Digital Rights Ireland and others [2014] CJEU Cases C-293/12 and C-594/12.

Fressoz and Roire v France [1999] ECHR Application no. 29183/95.

I v Finland [2008] ECHR Application no. 20511/03.

La Quadrature du Net [2020] CJEU Cases C-511/18, C-512/18 and C-520/18.

Magyar Helsinki Bizottság v Hungary [2016] ECHR Application no. 18030/11.

Roman Zakharov v Russia [2015] ECHR Application no. 47143/06.

S and Marper v United Kingdom [2008] ECHR Applications nos. 30562/04 and 30566/04.

Stankiewicz and others v Poland [2014] ECHR Application no. 48723/07.

Steel and Morris v United Kingdom [2005] ECHR Application no. 68416/01.

Szabó and Vissy v Hungary [2016] ECHR Application no. 37138/14.

Explanations Relating to the Charter of Fundamental Rights [2007].

Universal Declaration of Human Rights [1948].

https://doi.org/10.1017/qut.2024.2 Published online by Cambridge University Press