I think that computer based voting is a bad idea, simply because the stakes are too high. Even if the system in question is shown to be really secure and reliable, unless it can be rigorously proven to be foolproof, it is not worth the risk. Democracy is the prime asset that needs to be protected in a civilised world. This argument may (arguably) not feel that valid when talking about university elections, but the same principles can be extended to provincial or federal elections.

Tom Scott, a programmer and a YouTuber, made a [video](https://www.youtube.com/watch?v=w3_0x6oaDmI) in collaboration with the channel Computerphile explaining some of the key issues with using computer systems for voting, and he has a very interesting take on it. Favouring physical voting, he argues that the process is centuries old, fraud methods have been conceived and attempted, and the corresponding protection mechanisms have been devised in this time. There are two main factors that make physical voting much more secure: there is mandatory anonymity, and thus no one can be forced or bribed to change their vote; and a complete lack of trust among the opponents, which results in the counting process being totally transparent and the competitors keeping a natural check on each other. Attacks on physical voting, hence, do not scale well in comparison to attacks on computer based voting systems.

Scott then explains the issues with computer based voting by dividing the voting process into three parts: the use of the ballot software for recording votes; transferring the votes to the central counting system; and the central counting system itself. I would recommend the reader to watch the video for the details, but the main takeaway is that the mere fact that the entire process revolves around feeding raw data into a black-box and trusting it to correctly produce results deprives e-voting of the above mentioned security factors that physical voting has. To compare how dangerous this is, he compares the same process with the computers replaced by telephone operators: you phone some random stranger to cast your vote, and trust that he will pass on your message properly; that person will then send the vote to the central counter person reliably and anonymously; and the central counter will magically announce who the winner is. This is essentially parallel to what e-voting would be like. With smart people having trillions of dollars’ worth of motivation motivating them to design these attacks, these black-boxed stages are highly likely to be compromised.